AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Western District of Texas - Waco Division on the following

☐ Trademarks or ☒ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:22-cv-01094	October 21, 2022	Western District of Texas - Waco Division

PLAINTIFF	DEFENDANT
Taasera Licensing LLC	CrowdStrike, Inc. and CrowdStrike Holdings, Inc.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 7,673,137	3/2/2010	Taasera Licensing LLC
2 8,327,441	12/4/2012	Taasera Licensing LLC
3 8,850,517	9/30/2014	Taasera Licensing LLC
4 8,955,038	2/10/2015	Taasera Licensing LLC
5 8,990,948	3/24/2015	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 9,092,616	7/28/2015	Taasera Licensing LLC
2 9,608,997	3/28/2017	Taasera Licensing LLC
3 9,923,918	3/20/2018	Taasera Licensing LLC
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00427	10/31/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	MUSARUBRA US LLC, D/B/A TRELLIX

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	7,673,137	3/2/2010	Taasera Licensing LLC
2	8,327,441	12/4/2012	Taasera Licensing LLC
3	8,850,517	9/30/2014	Taasera Licensing LLC
4	8,955,038	2/10/2015	Taasera Licensing LLC
5	8,990,948	3/24/2015	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00427	10/31/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	MUSARUBRA US LLC, D/B/A TRELLIX

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	9,071,518	6/30/2015	Taasera Licensing LLC
2	9,092,616	7/28/2015	Taasera Licensing LLC
3	9,608,997	3/28/2017	Taasera Licensing LLC
4	9,923,918	3/20/2018	Taasera Licensing LLC
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00415	10/21/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	FORTINET INC.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 8,327,441	12/4/2012	Taasera Licensing LLC
2 8,819,419	8/26/2014	Taasera Licensing LLC
3 8,955,038	2/10/2015	Taasera Licensing LLC
4 8,990,948	3/24/2015	Taasera Licensing LLC
5 9,092,616	7/28/2015	Taasera Licensing LLC

In the above---entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above---entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1---Upon initiation of action, mail this copy to Director **Copy 3---Upon termination of action, mail this copy to Director**
Copy 2---Upon filing document adding patent(s), mail this copy to Director **Copy 4---Case file copy**

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00415	10/21/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	FORTINET INC.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 9,118,634	8/25/2015	Taasera Licensing LLC
2 9,608,997	3/28/2017	Taasera Licensing LLC
3 9,628,453	4/18/2017	Taasera Licensing LLC
4 9,860,251	1/2/2018	Taasera Licensing LLC
5 9,923,918	3/20/2018	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00063	2/25/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	CHECK POINT SOFTWARE TECHNOLOGIES LTD.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,842,796	1/11/2005	Taasera Licensing LLC
2 8,327,441	12/4/2012	Taasera Licensing LLC
3 8,955,038	2/10/2015	Taasera Licensing LLC
4 8,990,948	3/24/2015	Taasera Licensing LLC
5 9,092,616	7/28/2015	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00063	2/25/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	CHECK POINT SOFTWARE TECHNOLOGIES LTD.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 9,608,997	3/28/2017	Taasera Licensing LLC
2 9,923,918	3/20/2018	Taasera Licensing LLC
3		
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00062	2/25/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	PALO ALTO NETWORKS, INC.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,842,796	1/11/2005	Taasera Licensing LLC
2 7,673,137	3/2/2010	Taasera Licensing LLC
3 8,127,356	2/28/2012	Taasera Licensing LLC
4 8,327,441	12/4/2012	Taasera Licensing LLC
5 8,850,517	9/30/2014	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00062	2/25/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	PALO ALTO NETWORKS, INC.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 8,955,038	2/10/2015	Taasera Licensing LLC
2 8,990,948	3/24/2015	Taasera Licensing LLC
3 9,092,616	7/28/2015	Taasera Licensing LLC
4 9,923,918	3/20/2018	Taasera Licensing LLC
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00063	2/25/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	CHECK POINT SOFTWARE TECHNOLOGIES LTD.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,842,796	1/11/2005	Taasera Licensing LLC
2 8,327,441	12/4/2012	Taasera Licensing LLC
3 8,955,038	2/10/2015	Taasera Licensing LLC
4 8,990,948	3/24/2015	Taasera Licensing LLC
5 9,092,616	7/28/2015	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00063	2/25/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	CHECK POINT SOFTWARE TECHNOLOGIES LTD.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 9,608,997	3/28/2017	Taasera Licensing LLC
2 9,923,918	3/20/2018	Taasera Licensing LLC
3		
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Southern District of New York on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
22cv2306	3/22/2022	for the Southern District of New York

PLAINTIFF	DEFENDANT
PALO ALTO NETWORKS, INC.	TAASERA LICENSING LLC, and QUEST PATENT RESEARCH CORPORATION

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	6,842,796	1/11/2005	Taasera Licensing LLC
2	7,673,137	3/2/2010	Taasera Licensing LLC
3	8,127,356	2/28/2012	Taasera Licensing LLC
4	8,327,441	12/4/2012	Taasera Licensing LLC
5	8,850,517	9/30/2014	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
RUBY J. KRAJICK	/S/ V. BRAHIMI	3/23/2022

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

Trend Micro, Inc.
EX1002-12

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Southern District of New York on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
22cv2306	3/22/2022	for the Southern District of New York

PLAINTIFF	DEFENDANT
PALO ALTO NETWORKS, INC.	TAASERA LICENSING LLC, and QUEST PATENT RESEARCH CORPORATION

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 8,955,038	2/10/2015	Taasera Licensing LLC
2 8,990,948	3/24/2015	Taasera Licensing LLC
3 9,902,616	7/28/2015	Taasera Licensing LLC
4 9,923,918	3/20/2018	Taasera Licensing LLC
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
Ruby J. KRAJICK	/S/ V. BRAHIMI	3/23/2022

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00062	2/25/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	PALO ALTO NETWORKS, INC.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,842,796	1/11/2005	Taasera Licensing LLC
2 7,673,137	3/2/2010	Taasera Licensing LLC
3 8,127,356	2/28/2012	Taasera Licensing LLC
4 8,327,441	12/4/2012	Taasera Licensing LLC
5 8,850,517	9/30/2014	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
David A. O'Toole	nkl	3/22/22

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

Trend Micro, Inc.
EX1002-14

AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00062	2/25/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	PALO ALTO NETWORKS, INC.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 8,955,038	2/10/2015	Taasera Licensing LLC
2 8,990,948	3/24/2015	Taasera Licensing LLC
3 9,092,616	7/28/2015	Taasera Licensing LLC
4 9,923,918	3/20/2018	Taasera Licensing LLC
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

In light of the Notice, which the Court ACCEPTS AND ACKNOWLEDGES, and pursuant to Rule 41(a)(1)(A)(i), all pending claims and causes of action in the above-captioned case are DISMISSED WITHOUT PREJUDICE

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00063	2/25/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	CHECK POINT SOFTWARE TECHNOLOGIES LTD.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	6,842,796	1/11/2005	Taasera Licensing LLC
2	8,327,441	12/4/2012	Taasera Licensing LLC
3	8,955,038	2/10/2015	Taasera Licensing LLC
4	8,990,948	3/24/2015	Taasera Licensing LLC
5	9,092,616	7/28/2015	Taasera Licensing LLC

In the above---entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above---entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1---Upon initiation of action, mail this copy to Director Copy 3---Upon termination of action, mail this copy to Director
Copy 2---Upon filing document adding patent(s), mail this copy to Director Copy 4---Case file copy

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00063	2/25/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	CHECK POINT SOFTWARE TECHNOLOGIES LTD.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	9,608,997	3/28/2017	Taasera Licensing LLC
2	9,923,918	3/20/2018	Taasera Licensing LLC
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

Trend Micro, Inc.
EX1002-17

AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00062	2/25/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	PALO ALTO NETWORKS, INC.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,842,796	1/11/2005	Taasera Licensing LLC
2 7,673,137	3/2/2010	Taasera Licensing LLC
3 8,127,356	2/28/2012	Taasera Licensing LLC
4 8,327,441	12/4/2012	Taasera Licensing LLC
5 8,850,517	9/30/2014	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

Trend Micro, Inc.
EX1002-18

AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00062	2/25/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	PALO ALTO NETWORKS, INC.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 8,955,038	2/10/2015	Taasera Licensing LLC
2 8,990,948	3/24/2015	Taasera Licensing LLC
3 9,092,616	7/28/2015	Taasera Licensing LLC
4 9,923,918	3/20/2018	Taasera Licensing LLC
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:21-cv-00441	11/30/2021	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	TREND MICRO INCORPORATED

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	6,842,796	1/11/2005	Taasera Licensing LLC
2	7,673,137	3/2/2010	Taasera Licensing LLC
3	8,327,441	12/4/2012	Taasera Licensing LLC
4	8,850,517	9/30/2014	Taasera Licensing LLC
5	8,955,038	2/10/2015	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:21-cv-00441	11/30/2021	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	TREND MICRO INCORPORATED

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,990,948	3/24/2015	Taasera Licensing LLC
2	9,092,616	7/28/2015	Taasera Licensing LLC
3	9,608,997	3/28/2017	Taasera Licensing LLC
4	9,923,918	3/20/2018	Taasera Licensing LLC
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:21-cv-00441	11/30/2021	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	TREND MICRO INCORPORATED

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	6,842,796	1/11/2005	Taasera Licensing LLC
2	7,673,137	3/2/2010	Taasera Licensing LLC
3	8,327,441	12/4/2012	Taasera Licensing LLC
4	8,850,517	9/30/2014	Taasera Licensing LLC
5	8,955,038	2/10/2015	Taasera Licensing LLC

In the above---entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above---entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1---Upon initiation of action, mail this copy to Director Copy 3---Upon termination of action, mail this copy to Director
Copy 2---Upon filing document adding patent(s), mail this copy to Director Copy 4---Case file copy

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:21-cv-00441	11/30/2021	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	TREND MICRO INCORPORATED

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,990,948	3/24/2015	Taasera Licensing LLC
2	9,092,616	7/28/2015	Taasera Licensing LLC
3	9,608,997	3/28/2017	Taasera Licensing LLC
4	9,923,918	3/20/2018	Taasera Licensing LLC
5			

In the above---entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above---entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1---Upon initiation of action, mail this copy to Director Copy 3---Upon termination of action, mail this copy to Director
Copy 2---Upon filing document adding patent(s), mail this copy to Director Copy 4---Case file copy

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/399,065	12/04/2012	8327441	0079152-000002	3713

21839 7590 11/14/2012
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Srinivas KUMAR, Cupertino, CA;
Gurudatt Shashikumar, Foster City, CA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

21839 7590 09/17/2012
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/399,065	02/17/2012	Srinivas KUMAR	0079152-000002	3713

TITLE OF INVENTION: SYSTEM AND METHOD FOR APPLICATION ATTESTATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$870	$0	$0	$870	12/17/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
CERVETTI, DAVID GARCIA	2436	726-022000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 BUCHANAN INGERSOLL & ROONEY PC
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: TAASERA, INC.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): ERIE, PENNSYLVANIA

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
☒ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☒ Advance Order - # of Copies 2

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
☐ A check is enclosed.
☒ Payment by credit card.
☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 02-4800 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature [signature] Date November 2, 2012

Typed or printed name Charles F. Weiland III Registration No. 33,096

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Trend Micro, Inc.
EX1002-25

Electronic Patent Application Fee Transmittal

Application Number:	13399065
Filing Date:	17-Feb-2012
Title of Invention:	SYSTEM AND METHOD FOR APPLICATION ATTESTATION
First Named Inventor/Applicant Name:	Srinivas KUMAR
Filer:	Charles F. Wieland III/Roberto Negron
Attorney Docket Number:	0079152-000002

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl issue fee	2501	1	885	885
Extension-of-Time:				

Trend Micro, Inc.
EX1002-26

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Printed copy of patent - no color	8001	2	3	6
		Total in USD ($)		**891**

Electronic Acknowledgement Receipt

EFS ID:	14132703
Application Number:	13399065
International Application Number:	
Confirmation Number:	3713
Title of Invention:	SYSTEM AND METHOD FOR APPLICATION ATTESTATION
First Named Inventor/Applicant Name:	Srinivas KUMAR
Customer Number:	21839
Filer:	Charles F. Wieland III/Roberto Negron
Filer Authorized By:	Charles F. Wieland III
Attorney Docket Number:	0079152-000002
Receipt Date:	02-NOV-2012
Filing Date:	17-FEB-2012
Time Stamp:	10:25:25
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$891
RAM confirmation Number	7866
Deposit Account	024800
Authorized User	WIELAND, CHARLES F.

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	Fees_Transmittal.pdf	76281 db89afea340e571bb872fa0eb84c1c8272c9fb29	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	32113 c58c25d04f5fd9f12271460bcd95905409b9eb4a	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	108394		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/399,065	02/17/2012	Srinivas KUMAR	0079152-000002	3713

21839 7590 10/18/2012
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER
CERVETTI, DAVID GARCIA

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
10/18/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com
offserv@bipc.com

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address : COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
13/399,065	17 February, 2012	KUMAR ET AL.	0079152-000002

		EXAMINER	
BUCHANAN, INGERSOLL & ROONEY PC POST OFFICE BOX 1404 ALEXANDRIA, VA 22313-1404		David García Cervetti	
		ART UNIT	PAPER
		2436	20121011

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

The IDS filed 9/20/2012 has been considered.

/David García Cervetti/
Primary Examiner, Art Unit 2436

PTO-90C (Rev.04-03)

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13399065
Filing Date	2012-02-17
First Named Inventor	Srinivas KUMAR et al.
Art Unit	2436
Examiner Name	CERVETTI, DAVID GARCIA
Attorney Docket Number	0079152-000002

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20050289072	A1	2005-12-29	Sabharwal	
	2	20070143474	A1	2007-06-21	Sheng et al.	
	3	20070174406	A1	2007-07-26	Morris et al.	
	4	20090094584	A1	2009-04-09	Dheap et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH./DGC/

Receipt date: 09/20/2012	Application Number	13399065 13399065 - GAU: 2436
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2012-02-17
	First Named Inventor	Srinivas KUMAR et al.
	Art Unit	2436
	Examiner Name	CERVETTI, DAVID GARCIA
	Attorney Docket Number	0079152-000002

	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Notification of Transmittal of the International Search Report (Forms PCT/ISA/220 and PCT/ISA/210) and the Written Opinion of the International Searching Authority (Form PCT/ISA/237) dated August 27, 2012, issued in corresponding International Application No. PCT/US2012/025551. (9 pages)	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/David Garcia Cervetti/	Date Considered	10/11/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

Receipt date: 09/20/2012	Application Number	13399065 13399065 - GAU: 2436
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2012-02-17
	First Named Inventor	Srinivas KUMAR et al.
	Art Unit	2436
	Examiner Name	CERVETTI, DAVID GARCIA
	Attorney Docket Number	0079152-000002

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Charles F. Wieland III/	Date (YYYY-MM-DD)	2012-09-20
Name/Print	Charles F. Wieland III	Registration Number	33,096

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13399065
Filing Date	2012-02-17
First Named Inventor	Srinivas KUMAR et al.
Art Unit	2436
Examiner Name	CERVETTI, DAVID GARCIA
Attorney Docket Number	0079152-000002

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20050289072	A1	2005-12-29	Sabharwal	
	2	20070143474	A1	2007-06-21	Sheng et al.	
	3	20070174406	A1	2007-07-26	Morris et al.	
	4	20090094584	A1	2009-04-09	Dheap et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13399065
	Filing Date	2012-02-17
	First Named Inventor	Srinivas KUMAR et al.
	Art Unit	2436
	Examiner Name	CERVETTI, DAVID GARCIA
	Attorney Docket Number	0079152-000002

	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Notification of Transmittal of the International Search Report (Forms PCT/ISA/220 and PCT/ISA/210) and the Written Opinion of the International Searching Authority (Form PCT/ISA/237) dated August 27, 2012, issued in corresponding International Application No. PCT/US2012/025551. (9 pages)	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13399065
	Filing Date	2012-02-17
	First Named Inventor	Srinivas KUMAR et al.
	Art Unit	2436
	Examiner Name	CERVETTI, DAVID GARCIA
	Attorney Docket Number	0079152-000002

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Charles F. Wieland III/	Date (YYYY-MM-DD)	2012-09-20
Name/Print	Charles F. Wieland III	Registration Number	33,096

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	13399065
Filing Date:	17-Feb-2012
Title of Invention:	SYSTEM AND METHOD FOR APPLICATION ATTESTATION
First Named Inventor/Applicant Name:	Srinivas KUMAR
Filer:	Charles F. Wieland III/mich sok
Attorney Docket Number:	0079152-000002

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt

EFS ID:	13797430
Application Number:	13399065
International Application Number:	
Confirmation Number:	3713
Title of Invention:	SYSTEM AND METHOD FOR APPLICATION ATTESTATION
First Named Inventor/Applicant Name:	Srinivas KUMAR
Customer Number:	21839
Filer:	Charles F. Wieland III/mich sok
Filer Authorized By:	Charles F. Wieland III
Attorney Docket Number:	0079152-000002
Receipt Date:	20-SEP-2012
Filing Date:	17-FEB-2012
Time Stamp:	15:36:19
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$180
RAM confirmation Number	2355
Deposit Account	024800
Authorized User	WIELAND, CHARLES F.

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	PTO_SB08.PDF	612425 c38a3730d43f337c7211b0ac06fcb2d1481dd503	no	4
Warnings:					
Information:					
2	Non Patent Literature	NPL.pdf	407881 6ac04cbad2df17d4c46a4342d3bca785c749ce64	no	9
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30421 bd8388870e9c814e56f0488dd417dcb82d4b10ef	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1050727		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

21839 7590 09/17/2012
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER
CERVETTI, DAVID GARCIA

ART UNIT	PAPER NUMBER
2436	

DATE MAILED: 09/17/2012

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/399,065	02/17/2012	Srinivas KUMAR	0079152-000002	3713

TITLE OF INVENTION: SYSTEM AND METHOD FOR APPLICATION ATTESTATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$870	$0	$0	$870	12/17/2012

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 02/11)

Trend Micro, Inc.
EX1002-44

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

21839 7590 09/17/2012
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/399,065	02/17/2012	Srinivas KUMAR	0079152-000002	3713

TITLE OF INVENTION: SYSTEM AND METHOD FOR APPLICATION ATTESTATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$870	$0	$0	$870	12/17/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
CERVETTI, DAVID GARCIA	2436	726-022000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
   - ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
   - ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
   (1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
   (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
   1_____
   2_____
   3_____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): (**Please first reapply any previously paid issue fee shown above**)
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
- ❑ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/399,065	02/17/2012	Srinivas KUMAR	0079152-000002	3713

21839 7590 09/17/2012
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER
CERVETTI, DAVID GARCIA

ART UNIT	PAPER NUMBER
2436	

DATE MAILED: 09/17/2012

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 0 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 0 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Trend Micro, Inc.
EX1002-46

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No.	Applicant(s)	
	13/399,065	KUMAR ET AL.	
	Examiner	Art Unit	
	David García Cervetti	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *6/29/2012*.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are *1-26*.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 6/29/12
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/David García Cervetti/
Primary Examiner, Art Unit 2436

Trend Micro, Inc.
EX1002-48

DETAILED ACTION

1. Applicant's amendment filed 6/29/2012 has been fully considered.

2. Claims 1-26 are pending and have been examined.

Response to Amendment

3. This communication warrants No Examiner's Reason for Allowance, applicant's reply makes evident the reasons for allowance, satisfying the "record as a whole" proviso of the rule 37 CFR 1.104(e). Specifically, applicant's arguments filed on 6/29/2012 are persuasive, as such the reasons for allowance are in all probability evident from the record and no statement is deemed necessary (see MPEP 1302.14).

Allowable Subject Matter

4. Claims 1-26 are allowed.

5. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David García Cervetti whose telephone number is (571)272-5861. The examiner can normally be reached on Monday-Friday 8 AM to 5 PM.
7. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Philip J. Chea can be reached on (571)272-3951. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.
8. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/David García Cervetti/
Primary Examiner, Art Unit 2436

Notice of References Cited	Application/Control No. 13/399,065	Applicant(s)/Patent Under Reexamination KUMAR ET AL.	
	Examiner David García Cervetti	Art Unit 2436	Page 1 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,091,835 A	07-2000	Smithies et al.	382/115
*	B	US-6,507,904 B1	01-2003	Ellison et al.	712/229
*	C	US-6,760,441 B1	07-2004	Ellison et al.	380/45
*	D	US-2005/0033987 A1	02-2005	Yan et al.	713/201
*	E	US-2005/0132202 A1	06-2005	Dillaway et al.	713/179
*	F	US-2005/0132031 A1	06-2005	Sailer et al.	709/223
*	G	US-2005/0138384 A1	06-2005	Brickell et al.	713/182
*	H	US-2005/0221766 A1	10-2005	Brizek et al.	455/073
*	I	US-2005/0283660 A1	12-2005	McKeen et al.	714/011
*	J	US-6,990,579 B1	01-2006	Herbert et al.	713/164
*	K	US-2006/0005009 A1	01-2006	Ball et al.	713/155
*	L	US-6,996,710 B1	02-2006	Ellison et al.	713/156
*	M	US-7,013,481 B1	03-2006	Ellison et al.	726/4

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Trend Micro, Inc.
EX1002-51

Notice of References Cited	Application/Control No. 13/399,065	Applicant(s)/Patent Under Reexamination KUMAR ET AL.	
	Examiner David García Cervetti	Art Unit 2436	Page 2 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2006/0200680 A1	09-2006	Ellison et al.	713/190
*	B	US-2007/0005992 A1	01-2007	Schluessler et al.	713/193
*	C	US-7,194,759 B1	03-2007	Chess et al.	726/2
*	D	US-2007/0185856 A1	08-2007	Mittal et al.	707/005
*	E	US-2008/0015808 A1	01-2008	Wilson et al.	702/123
*	F	US-2008/0083039 A1	04-2008	CHOI et al.	726/27
*	G	US-2008/0141027 A1	06-2008	Kim et al.	713/156
*	H	US-2008/0235372 A1	09-2008	Sailer et al.	709/224
*	I	US-2008/0289028 A1	11-2008	Jansen et al.	726/11
*	J	US-2009/0178138 A1	07-2009	Weiss et al.	726/22
*	K	US-2009/0172814 A1	07-2009	Khosravi et al.	726/23
*	L	US-2009/0204964 A1	08-2009	Foley et al.	718/1
*	M	US-2009/0204806 A1	08-2009	Kanemura et al.	713/155

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Trend Micro, Inc.
EX1002-52

Notice of References Cited	Application/Control No. 13/399,065	Applicant(s)/Patent Under Reexamination KUMAR ET AL.	
	Examiner David García Cervetti	Art Unit 2436	Page 3 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,587,607 B2	09-2009	Brickell et al.	713/182
*	B	US-7,797,544 B2	09-2010	Dillaway et al.	713/179
*	C	US-2010/0281273 A1	11-2010	Lee et al.	713/190
*	D	US-2011/0035577 A1	02-2011	Lin et al.	713/150
*	E	US-7,882,221 B2	02-2011	Sailer et al.	709/224
*	F	US-2011/0154500 A1	06-2011	Sahita et al.	726/26
*	G	US-7,984,304 B1	07-2011	Waldspurger et al.	713/187
*	H	US-2011/0173643 A1	07-2011	Nicolson et al.	719/328
*	I	US-7,979,696 B2	07-2011	Kim et al.	713/156
*	J	US-2011/0179477 A1	07-2011	Starnes et al.	726/9
*	K	US-8,108,536 B1	01-2012	Hernacki et al.	709/231
*	L	US-2012/0084850 A1	04-2012	Novak et al.	726/8
*	M	US-2012/0131334 A1	05-2012	Haikney et al.	713/156

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Trend Micro, Inc.
EX1002-53

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	2	(US-20090172814-$ or US-20070005992-$).did.	US-PGPUB	OR	OFF	2012/09/06 11:43
L3	2	("20090172814" "20070005992").pn. and (binary binaries hash digest load loaded loading child parent process)	US-PGPUB	OR	OFF	2012/09/06 11:45
L4	13	(web near3 application servlet) near8 (child parent) near6 process	US-PGPUB	OR	ON	2012/09/06 11:56
L5	23	(web near3 application servlet) near8 (child parent) near6 process	US-PGPUB; USPAT	OR	ON	2012/09/06 11:56
L6	3	(web near3 application servlet) near8 (child parent) and (web near3 application servlet) near8 (signature digest hash hashing signing hashed)	US-PGPUB; USPAT	OR	ON	2012/09/06 12:00
L7	106	(web near3 application servlet) near8 (child parent) and (signature digest hash hashing signing hashed)	US-PGPUB; USPAT	OR	ON	2012/09/06 12:05
L8	24	(web near3 application servlet) near8 (child parent) and (signature digest hash hashing signing hashed) near8 (program software application servlet)	US-PGPUB; USPAT	OR	ON	2012/09/06 12:06
L9	3944	execution near6 (analysis analysing analyzed) near8 (file application program software)	US-PGPUB; USPAT	OR	ON	2012/09/06 12:14
L10	1	execution near6 (analysis analysing analyzed) near8 (file application program software) and (runtime run adj time execuction near3 time) near8 (attest$)	US-PGPUB; USPAT	OR	ON	2012/09/06 12:15
L11	1	execution near6 (analysis analysing analyzed) near8 (file application program software) and (runtime run adj time execuction near3 time) and (attest$)	US-PGPUB; USPAT	OR	ON	2012/09/06 12:15
L12	26	mutual near6 attestation	US-PGPUB; USPAT	OR	ON	2012/09/06 12:22
L13	32	(attestation attest attesting) near6 parent near6 child	US-PGPUB; USPAT	OR	ON	2012/09/06 12:33
L14	3625	726/22.ccls.	US-PGPUB; USPAT	OR	ON	2012/09/06 12:34
S1	3286	726/22.ccls.	US-PGPUB; USPAT	OR	OFF	2012/04/11 23:30
S2	2280	726/23.ccls.	US-PGPUB; USPAT	OR	OFF	2012/04/11 23:30

S3	1855	726/24.ccls.	US-PGPUB; USPAT	OR	OFF	2012/04/11 23:30
S4	1422	726/25.ccls.	US-PGPUB; USPAT	OR	OFF	2012/04/11 23:30
S5	167	(runtime execution executing) near7 (attest$)	US-PGPUB; USPAT	OR	OFF	2012/04/11 23:39
S6	20	(runtime execution executing) near7 (attest$) near8 server	US-PGPUB; USPAT	OR	OFF	2012/04/11 23:39
S7	62	(runtime execution executing) near5 (application context program) and (attest$) near8 server	US-PGPUB; USPAT	OR	OFF	2012/04/11 23:42
S8	1	"7540030".pn.	US-PGPUB; USPAT	OR	OFF	2012/04/12 09:22
S9	1	"20030212906".pn.	US-PGPUB; USPAT	OR	OFF	2012/04/12 09:22
S10	1	"7540030".pn. and (log logfile record)	US-PGPUB; USPAT	OR	OFF	2012/04/12 09:24
S11	1	"20030212906".pn. and (log logfile record)	US-PGPUB; USPAT	OR	OFF	2012/04/12 09:25
S12	38	(application program) near5 attest$ and (attest$) near8 server	US-PGPUB; USPAT	OR	OFF	2012/04/12 14:47
S13	1	"20110179477".pn.	US-PGPUB; USPAT	OR	OFF	2012/09/05 22:37
S14	1	"20120216244".pn. and (child parent)	US-PGPUB; USPAT	OR	OFF	2012/09/05 23:21
S15	1	"20110179477".pn. and (parent child)	US-PGPUB; USPAT	OR	OFF	2012/09/05 23:25
S16	1	"20110179477".pn. and (process)	US-PGPUB; USPAT	OR	OFF	2012/09/05 23:26
S17	6	("20090133110" | "20090138939" | "20090144818" | "20090241170" | "20090276204" | "20090328186").PN.	US-PGPUB; USPAT	OR	OFF	2012/09/05 23:43
S18	1	("20090133110" | "20090138939" | "20090144818" | "20090241170" | "20090276204" | "20090328186").PN. and (token attest$)	US-PGPUB; USPAT	OR	OFF	2012/09/05 23:44
S19	34533	execution near6 state	US-PGPUB; USPAT	OR	OFF	2012/09/05 23:46
S20	265	runtime near6 execution near6 state	US-PGPUB; USPAT	OR	OFF	2012/09/05 23:46
S21	462	runtime near6 execution near6 (state context)	US-PGPUB;	OR	OFF	2012/09/05 23:47

			USPAT			
S22	38	runtime near6 execution near6 (state context) same3 (attribute binaries)	US-PGPUB; USPAT	OR	OFF	2012/09/05 23:48
S23	462	runtime near6 execution near6 (state context)	US-PGPUB; USPAT	OR	OFF	2012/09/05 23:52
S24	1	runtime near6 execution near6 (state context) and (attest attestation)	US-PGPUB; USPAT	OR	OFF	2012/09/05 23:52
S25	163	(runtime execution) near6 (state context) and (attest attestation)	US-PGPUB; USPAT	OR	OFF	2012/09/05 23:53
S26	68	(runtime execution) near6 (state context) and (attest attestation) and ((file application program software) near4 (hash signature))	US-PGPUB; USPAT	OR	OFF	2012/09/05 23:54

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L15	15	(attestation attest attesting) near6 parent near6 child	USPAT; UPAD	OR	ON	2012/09/06 12:34
L16	34	(runtime execution) near6 (state context) and (attest attestation) and ((file application program software) near4 (hash signature))	USPAT; UPAD	OR	OFF	2012/09/06 12:34
L17	18	runtime near6 execution near6 (state context) same3 (attribute binaries)	USPAT; UPAD	OR	OFF	2012/09/06 12:35
L18	13	(application program) near5 attest$ and (attest$) near8 server	USPAT; UPAD	OR	OFF	2012/09/06 12:35
L19	12	(web near3 application servlet) near8 (child parent) and (signature digest hash hashing signing hashed) near8 (program software application servlet)	USPAT; UPAD	OR	ON	2012/09/06 12:35

9/6/2012 12:37:10 PM
H:\Workspaces\Workspaces\13-399-065-04-11-2012.wsp

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	**13/399,065**
Filing Date	**February 17, 2012**
First Named Inventor	**Kumar, Srinivas**
Art Unit	**2436**
Examiner Name	**Cervetti, David Garcia**
Attorney Docket Number	**0079152-000002**

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (*if known*)		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2009/0144818	A1	06-04-2009	Kumar *et al.*.	
		US-2009/0138939	A1	05-28-2009	Kumar *et al.*	
		US-2009/0276204	A1	11-05-2009	Kumar *et al.*	
		US-2009/0241170	A1	09-24-2009	Kumar *et al.*	
		US-2009/0133110	A1	05-21-2009	Kumar *et al.*	
		US-2009/0328186	A1	12-31-2009	Pollutro *et al.*	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] (*if known*)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

Examiner Signature	/David Garcia Cervetti/	Date Considered	09/05/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional). 2 See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. 3 Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). 4 For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. 5 Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. 6 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DGC/

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13399065	KUMAR ET AL.
	Examiner	**Art Unit**
	David García Cervetti	2436

ORIGINAL		INTERNATIONAL CLASSIFICATION										
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED					
726	22	H	0	4	L	29 / 06 (2006.01.01)						

CROSS REFERENCE(S)					
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		17												
	2		18												
	3		19												
	4		20												
	5		21												
	6		22												
	7		23												
	8		24												
	9		25												
	10		26												
	11														
	12														
	13														
	14														
	15														
	16														

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	26	
/David García Cervetti/ Primary Examiner.Art Unit 2436	09/06/2012	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Trend Micro, Inc.
EX1002-58

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13399065	KUMAR ET AL.
	Examiner	**Art Unit**
	David García Cervetti	2436

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/11/2012	09/06/2012							
	1	✓	=							
	2	✓	=							
	3	✓	=							
	4	✓	=							
	5	✓	=							
	6	✓	=							
	7	✓	=							
	8	✓	=							
	9	✓	=							
	10	✓	=							
	11	✓	=							
	12	✓	=							
	13	✓	=							
	14	✓	=							
	15	✓	=							
	16	✓	=							
	17	✓	=							
	18	✓	=							
	19	✓	=							
	20	✓	=							
	21	✓	=							
	22	✓	=							
	23	✓	=							
	24	✓	=							
	25	✓	=							
	26	✓	=							

Trend Micro, Inc.
EX1002-59

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13399065	KUMAR ET AL.
	Examiner	**Art Unit**
	David García Cervetti	2436

SEARCHED

Class	Subclass	Date	Examiner
726	22,23,24,25	9/6/2012	DGC

SEARCH NOTES

Search Notes	Date	Examiner
inventor name search, acm, ieee, springer, google, scholar, east history attached	9/6/2012	DGC

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner
726	22,23,24,25	9/6/2012	DGC

	/David García Cervetti/ Primary Examiner.Art Unit 2436

Trend Micro, Inc.
EX1002-60

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/399,065	02/17/2012	Srinivas KUMAR	0079152-000002

CONFIRMATION NO. 3713

21839
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

PUBLICATION NOTICE

OC000000056138057

Title:SYSTEM AND METHOD FOR APPLICATION ATTESTATION

Publication No.US-2012-0216244-A1
Publication Date:08/23/2012

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Trend Micro, Inc.
EX1002-61

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	**MAIL STOP AMENDMENT**
Kumar, Srinivas et al.	Group Art Unit: 2436
Application No.: 13/399,065	Examiner: Cervetti, David Garcia
Filed: February 17, 2012	Confirmation No.: 3713
For: System and Method for Application Attestation	

AMENDMENT AND REPLY UNDER 37 C.F.R. § 1.111

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In reply to the Office Action dated April 27, 2012, Applicants submit the following Amendment and Remarks.

Amendments to the Specification begin on page 2 of this paper. Amendments to the Claims are reflected in the listing of claims, which begins on page 4 of this paper.

Remarks and Arguments begin on page 15 of this paper.

It is not believed that extensions of time or fees for net addition of claims are required beyond those that may otherwise be provided for in documents accompanying this paper. However, if additional extensions of time are necessary to prevent abandonment of this application, then such extensions of time are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required therefore (including fees for net addition of claims) are hereby authorized to be charged to our Deposit Account No. 02-4800.

AMENDMENTS TO THE SPECIFICATION:

Kindly amend paragraph [0008] of the specification as follows:

The presently disclosed technology also may be embodied as an additional method, apparatus and/or system for a runtime monitor to inspect web and non-web applications (e.g., all web and non-web applications) running on the instrumented target platform. The system may include an attestation service (or broker) using an attestation server and configured to generate application artifacts and/or to issue application statements or claims. The application artifact may represent an identified application instance (e.g., at runtime, globally[[, uniquely]] unique, opaquely and/or in a time-sensitive manner, for example, using an application artifact having a specified or predetermined lifetime) on an instrumented platform (such as but not limited to a, Personal Digital Assistant (PDA), a tablet computing device, an iPhone™, an iPod™, an iPad™, a device operating the Android operating system (OS) from Google Inc., a device running the Microsoft Windows® Mobile OS, a device running the Microsoft Windows® Phone OS, a device running the Symbian OS, a device running the webOS from Hewlett Packard, Inc., a mobile phone, a BlackBerry® device, a smartphone, a hand held computer, a netbook computer, a palmtop computer, a laptop computer, an ultra-mobile PC, a portable gaming system, a gaming console, or another similar type of computing device having a computer, microprocessor). The application statements may include at least one statement (or claim) about an inspected runtime execution context and/or an intelligence based security context.

Kindly amend paragraph [0025] of the specification as follows:

In certain exemplary embodiments, ~~applicants~~ applications may be secured by signing-on or authenticating applications onto the network using an attestation process (e.g., via a single factor or multi-factor attestation). In a multi-factor process, applications may be qualified based on at least two factors. A first factor may identify one or more attributes of the application (e.g., run time instance of the application) such as (1) a hash of the application, as an application fingerprint, (2) other applications/processes called by the application, (3) ports used by the application, (4) computing, storage, and network resource usage by the application, and/or (5) the platform executing the application, among ~~other~~ others. Such information may be available locally (e.g., at the computing platform running the application) in the current execution context. A second factor may identify what is known about the application based on the attributes of the application from security intelligence external to the operating environment (e.g., a third party (e.g., trusted third party) separate from the computing platform running the application).

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A method of providing an attestation service for an application at runtime executing on a computing platform using an attestation server, comprising:

receiving, by the attestation server remote from the computing platform:

a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application; and

a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components;

generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result; and

sending, by the attestation server, the attestation result associated with the application.

2. (Original) The method of claim 1, further comprising:

generating, by the attestation server, an application artifact as a reference for changes in a subsequent execution context; and

sending the generated application artifact such that subsequent changes to the runtime execution context are tracked based on the generated application artifact.

3. (Currently Amended) The method according to claim 2, further comprising digitally signing the attestation results, ~~and the application artifact~~

wherein the attributes further comprise parent-child process associations of the application.

4. (Currently Amended) The method of claim 1, wherein the received security context is an introspective security context, and wherein the execution analysis is a static, dynamic, or virtual analysis of the one or more executable file binaries and the loaded components.

5. (Currently Amended) The method of claim [[1]] 4, wherein the generating of the report indicating security risks associated with the application includes generating, by the attestation server, one or more security assertions that pertain to the received runtime execution context and the received introspective security context.

6. (Original) The method according to claim 1, further comprising authenticating the application using a plurality of collaboration services.

7. (Original) The method according to claim 1, further comprising controlling a user's transaction with the application by applying a set of authorization rules in accordance with the attestation results.

8. (Original) The method according to claim 1, further comprising controlling a user's network access to the application by applying a set of authorization rules in accordance with the attestation results.

9. (Original) The method according to claim 1, further comprising providing confidence metrics in the attestation results indicating a level of security risk by different classifications such that a restriction on a user's transaction with the application are applied based on the level of security risk indicated by the confidence metrics in the attestation results.

10. (Original) The method according to claim 9, wherein the application of the restriction on the user's transaction includes applying the restriction on the user's network access to the application.

11. (Original) The method according to claim 1, wherein the application of the restriction on the user's transaction includes applying routing decisions and redirecting the user to an alternate computer platform.

12. (Original) The method according to claim 1, further comprising controlling, by a network access enforcer, access of a user to the application based on the attestation result.

13. (Currently Amended) A non-transitory computer readable medium having instructions stored thereon that, if executed by a computing device, cause the computing device to perform operations for providing mutual attestation of applications in client-server or peer-to-peer transactions using an attestation server, the operations comprising:

generating and sending, by the attestation server, a first application artifact that dynamically and opaquely identifies:

an instance of a first application; and

a record of a current execution state of the first application;

receiving and validating, by the attestation server, from a server in the client server transaction or from a first peer in the peer-to-peer transaction, the first application artifact sent by the attestation server to a client in a client server transaction or to a second peer in the peer-to-peer transaction;

generating and sending application statements to the client and the server or the first and second peers about interrelated applications used in the client-server or peer-to-peer transactions.

14. (Currently Amended) The computer readable medium of claim 13, the operations further comprising:

generating and sending, by the attestation server, a second application artifact that dynamically and opaquely identifies:

an instance of a second application; and

a record of a current execution state of the second application;

receiving and validating, by the attestation server, from a client in the client server transaction or from a second peer in the peer-to-peer transaction, the second application artifact sent by the attestation server to a server in a client server transaction or to a first peer in the peer-to-peer transaction.

15. (Currently Amended) The computer readable medium of claim 14, wherein:

[[the]] sending [[of]] the application statements ~~to the client and the server or the first and second peers~~ comprises the following operations:

sending, by the attestation server:

[[the]] an application statement regarding a client application of the interrelated applications to the server of the client-server transaction and the application statement regarding a server application of the interrelated applications to the client of the client-server transaction; or

[[the]] an application statement regarding a first peer application of the interrelated applications to the second peer of the peer-to-peer transaction and the application statement regarding a second peer application of the interrelated applications to the first peer of the peer-to-peer transaction; and

determining, based at least in part upon the sent application statements, whether or not to exchange ~~transact~~ data ~~exchanges~~ with associated applications.

16. (Currently Amended) The computer readable medium of claim 15, wherein:

[[the]] generating [[of]] the application statements ~~includes:~~ comprises including ~~in the application statements~~ confidence metrics and contextual assertions in the application statements; and

[[the]] determining ~~whether to transact data exchanges with the associated applications~~ includes:

comparing respective confidence metrics to a set of rules; and

determining whether or not to exchange ~~transact~~ data ~~exchange~~ based on the comparison.

17. (Currently Amended) A method for providing attestation of the authenticity of a running web application or web servlet using an attestation server, comprising:

requesting an application artifact that is a dynamic, opaque reference to [[for]] a running web application or servlet instance;

establishing a secure channel between the web server and the attestation server;

generating at least one ~~hash file digest~~ digital signature corresponding to the execution context of the web application or servlet instance;

determining at least one ~~file attribute~~ parent-child process association corresponding to ~~at least one element or~~ the execution context of the web application or web servlet instance;

sending an application report to an identity provider;

generating assertions based on a received security context and a received local execution context;

transmitting confidence metrics in the report to the identity provider; and

providing attestation of the running web application or web servlet as a digital icon for rendering by a web browser.

18. (Currently Amended) The method according to claim 17, wherein the ~~attestation~~ providing is ~~provided~~ prior to commencing any data exchange in an established connection with a user.

19. (Currently Amended) The method according to claim 17, wherein the ~~attestation~~ providing is ~~provided~~ prior to establishing a network connection with a user.

20. (Original) The method according to claim 19, further comprising rendering attestation information about the web application to be accessed responsive to user input.

21. (Currently Amended) A system for continuously monitoring running applications hosted on self-managed and on-premise, or on outsourced service provider managed infrastructure comprising:

an instrumented target platform for hosting [[a]] target, running applications ~~user or service program~~;

an application attestation service for:

generating [[a]] globally unique, opaque, and time-sensitive application ~~artifact~~ artifacts identifying records of current execution states and application statements for the target, running applications including a plurality of assertions pertaining to inspection based runtime local execution context and introspection based security context; and

remediating the instrumented target platform, wherein the remediating includes one or more of: a reimage, a snapshot, or a quarantine of the instrumented target platform;

a runtime monitor for:

discovering, identifying and inspecting running application processes on the instrumented target platform, wherein the discovering includes analysis of executable file binaries of the target, running applications; and

[[for]]generating metadata that includes at least the runtime local execution context;

a collaboration service configured to:

provide introspected security context for [[a]] the target, running applications ~~application running~~ on the instrumented target platform; and

analyze executable file binaries for the target application running on the instrumented target platform; and

a graphical user interface configured to:

request and receive dynamic assertions from a metadata repository of the attestation service, the dynamic assertions pertaining to the local execution context or the introspected security context of running application instances on the instrumented target platform ~~platforms~~;

continuously display the dynamic assertions ~~to a system administrator~~; and

provision and dispatch alerts based on the dynamic assertions and predefined criteria.

22. (Currently Amended) The system according to claim 21, ~~wherein~~ further comprising a network access enforcer configured to:

~~subscribes for~~ subscribe to and ~~receives~~ receive dynamic application statements including contextual assertions from an attestation service;

[[to]] analyze the contextual assertions; and

determine whether or not an authenticated user is permitted ~~or denied network~~ to access [[to]] an attested application instance via a network.

23. (Currently Amended) The system according to claim 21, wherein the graphical user interface ~~displays~~ is further configured to:

display the applications running on the instrumented target platform [[on]] in a client specific dashboard or portal, and

~~presents~~ present, for each associated application execution context, at least one of:

a service hostname;

a service realm;

a service principal name;

a product version;

a product vendor;

one or more ~~classifications~~ classification-based confidence metrics;

an active network service port; or

executable file binaries.

24. (Currently Amended) The system according to claim 21, further comprising an identity provider ~~that queries~~ configured to:

query for dynamic application statements from the attestation server including contextual assertions;

[[to]] analyze the contextual assertions; and

[[to]] determine whether or not an authenticated user is ~~permitted~~ authorized ~~or denied authorization~~ to ~~transact~~ exchange data ~~exchanges~~ with an attested application instance [[in]] via an established connection.

25. (Currently Amended) The system according to claim 21, further comprising a network access enforcer ~~that analyzes~~ configured to:

analyze classifications based confidence metrics included in received dynamic application statements, based on a subscription, from an attestation service; and

[[to]] determine whether or not an authenticated user is permitted ~~or denied network~~ to access [[to]] an attested application instance via a network.

26. (Currently Amended) The system according to claim 21, ~~wherein an~~ further comprising an identity provider ~~analyzes~~ configured to:

analyze ~~classifications~~ classification-based confidence metrics included in received dynamic application statements, based on a subscription, from an attestation service; and

[[to]] determine whether or not an authenticated user is ~~permitted or denied authorization~~ authorized to ~~transact~~ exchange data ~~exchanges~~ with an attested application instance [[in]] via an established connection.

REMARKS

Reconsideration of this Application is respectfully requested. Upon entry of the foregoing amendment, claims 1-26 are pending in the application, with claims 1, 13, 17 and 21 being independent claims. Claims 1, 3-5, 13-19 and 21-26 are amended to clarify Applicants' techniques. The specification is amended to correct typographical errors. Support for the amendments is found throughout the original specification, at least at, for example paragraphs [0008], [0009], [0012], [0019], [0025], [0031], [0033], [0036] - [0038], [0045], [0047], [0058], [0060], [0062], [0081], [0083], [0090], [0092]-[0095], [0097], [0098], [0115], [0127], [0132], [0137], [0141] and [0147] and FIG. 12 and originally filed claims 1, 13, 17 and 21.

Applicants reserve the right to prosecute similar or broader claims, with respect to the amended claims, in the future.

Based on the above amendment and the following remarks, Applicants respectfully request that the Examiner reconsider all outstanding rejections and that they be withdrawn.

Statement of Substance of Examiner Interview

Further to the Interview Summary dated June 14, 2012 (PTO Prosecution File Wrapper Paper No. 20120607, "the Examiner's interview summary"), Applicants submit the following Statement of Substance of Interview conducted between the Examiner, Applicant Srinivas Kumar, and Applicants' representatives, Charles F. Wieland and Randall K. Baldwin. Applicants and Applicants' representatives gratefully acknowledge the courtesies extended to them by the Examiner in granting a personal interview on June 7, 2012. During the Interview, the Examiner clarified

his comments regarding his interpretation of the teachings of the applied reference. In particular, the Examiner clarified his comments regarding claims 1, 13, 17 and 21 and his interpretation of the teachings of Starnes. In the interview, Applicants' representatives and the Examiner discussed the rejection of claim 21 and the Examiner agreed that the remediating recited in this claim is not disclosed in the portion of Starnes cited in the Office Action. Applicant and Applicants' representative discussed distinctions between independent claims 1, 13, 17 and 21 and Starnes with the Examiner. Applicants' representatives and the Examiner discussed suggested claim language to convey the aforementioned distinctions between the applied reference and the claims, but no specific agreement was reached. Additional substance of the discussion and arguments in the Interview is included in the present remarks.

Rejections Under 35 U.S.C. § 102

The Examiner rejected claims 1-26 under 35 U.S.C. 102(b) as allegedly being anticipated by U.S. Patent Publication No. 2011/0179477 to Starnes *et al.* ("Starnes"). Applicants respectfully traverse these rejections for the reasons stated below.

For a prior art reference to anticipate the claimed invention, it must disclose each and every element as set forth in the claim. *See, Finnigan Corp. v. United States Int'l Trade Comm'n*, 180 F.3d 1354, 1365-66 (Fed. Cir. 1999). The requirements of strict identity between the claim and the prior art reference, is not met if a single element or limitation required by the claim is missing from the prior art source. *See, Structural Rubber Prods. Co. v. Park Rubber Co.*, 749 F.2d 707,716 (Fed. Cir. 1984). Anticipation under 35 U.S.C. § 102 requires showing the presence

in a single reference disclosure of each and every element of the claimed invention, arranged as in the claim. See, *Lindemann Maschinenfabrik GMBH v. American Hoist & Derrick*, 221 U.S.P.Q. 481, 485 (Fed. Cir. 1984). Further, "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." See, *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987) and M.P.E.P. §2131. Applicants submit that this is not found using Starnes.

However, as discussed during the aforementioned interview, merely in order to expedite prosecution and without conceding the propriety of any rejection, Applicants have herein amended claims 1, 3, 13-19 and 21-26. Applicants respectfully submit that there are a number of patentable differences between Starnes and amended independent claims 1, 13, 17 and 21.

By way of example and not limitation, Applicants' specification describes that an "application artifact may represent an identified application instance . . . at runtime . . . in a time-sensitive manner . . . using an application artifact having a specified or predetermined lifetime" and "may include at least a registered name (e.g., a registered globally unique security principal name) for the running application instance (e.g., a user program or a service program, among others)." (Applicants' specification, paragraphs [0008] and [0012]). With reference to FIG. 1, the specification describes non-limiting embodiments wherein application artifacts 107 can "maintain a record of the state of the discovered or identified applications running on the instrumented platform 100 . . . for discovered or identified applications running on the instrumented platform 100" a "runtime monitor 102 may use the application artifacts 107 to generate attribute value assertions (e.g., assertions

regarding one or more attribute values associated with each respective running application" and an "application artifact may include previous assertions or may provide an identifier that associates the application to the previous assertions." (Applicants' specification, paragraphs [0033] and [0036]). With reference to the exemplary embodiment of FIG. 2, the specification describes a "dynamically changing application artifact 206 which may be time sensitive and may be globally unique" and "may be based on the received application execution context." (Applicants' specification, paragraph [0060]). Applicants' specification also describes exemplary embodiments for generating a "globally unique, opaque, time-sensitive application artifact." (Applicants' specification, paragraphs [0137], [0141] and [0147]).

The instant specification describes exemplary embodiments wherein "[r]esponsive to or after detection of application process start, a runtime application execution context (e.g., metadata) may be generated" and "may include . . . file attributes (for example, the file size, the publisher details, the creation and/or the modification timestamps, the digital signing, and/or the product version) for loaded components of the running target application, (3) parent-child process associations, (4) loader dependencies, and/or (5) information about active listening and/or open network ports that may be well-known and/or ephemeral; and/or executable file binaries." (Applicants' specification, paragraph [0058]). The specification describes that "attribute value assertions for the application execution context . . . may include file attributes (e.g., file size, publisher details, creation and/or modification timestamps, digital signings, and product versions) for loaded (e.g., all loaded and/or in process) components of the running target application . . . parent-child process

associations and/or loader dependencies, information about active listening and/or open network ports that are well known or ephemeral" and "may also include the executable file binaries." (Applicants' specification, paragraph [0037]). With reference to the exemplary embodiment of FIG. 5, the specification describes that "attributes of components of the running server application 501 including parent-child process associations and loader dependencies." (Applicants' specification, paragraph [0092]). Applicants' specification also describes an exemplary embodiment wherein the "the authenticity of the running application" can be verified "with a real time or near real time exchange 409 of the received metadata with one or more collaboration services 403 and the return of the application security context 410 based on the exchanged metadata" and "a static, dynamic and/or virtual execution analysis of the executable file binary." (Applicants' specification, paragraph [0081]).

Applicants have amended claim 1, 4, 13, 17 and 21 to broadly encompass the forgoing features.

For example, claim 1 as amended herein recites, *inter alia*, "a runtime execution context indicating attributes of the application at runtime, wherein ***the attributes comprise one or more executable file binaries of the application and loaded components of the application***" and "a security context providing security information about the application, wherein ***the security information comprises an execution analysis of the one or more executable file binaries and the loaded components***."

Also, for example, claims 13 and 21 recite, among other features: "generating and sending . . . a first application artifact that dynamically and opaquely identifies:

an instance of a first application; and a record of a current execution state of the first application" and "generating ***globally unique, opaque, and time-sensitive application artifacts identifying records of current execution states*** and application statements for the target, running applications," respectively.

Further, for example, claim 17 recites, *inter alia*:

> requesting ***an application artifact that is a dynamic, opaque reference to a running*** web ***application or*** servlet ***instance***;
> . . .
> generating at least one ***digital signature corresponding to the execution context of the*** web ***application or*** servlet ***instance***; [and]
> determining at least one ***parent-child process association corresponding to the execution context*** of the web application or web servlet instance[.]

Claim 1

On pages 2-3 of the Office Action, the Office alleges that Starnes discloses all of the features of claim 1. Specifically, the Office asserts that the features of claim 1 are disclosed in paragraphs [0017], [0023], and [0028] - [0029] of Starnes. Even assuming for the sake of argument that the Office's interpretation of the above-noted portions of Starnes is correct, which Applicants do not acquiesce to, Starnes is silent regarding the above-quoted distinguishing features of claim 1. At page 2 of the Office Action, with regard to previously-pending claim 1, the Office asserts that Starnes discloses a "runtime execution context indicating attributes of the application at runtime" at paragraph [0017], which discusses a system "configured to generate a one-time application token." Starnes discloses that "[t]he application token may include a digitally signed token . . .[t]he trust authentication broker may include a security token service (STS)" and "[t]he application token may be used by network access enforcers (e.g. firewalls), authentication brokers (e.g. security token service

(STS) and active clients (e.g. simple authentication and security layer (SASL) applications)." (Starnes, paragraphs [0009] and [0021]).

As discussed during the aforementioned interview, Starnes is directed to a system wherein a trust broker service generates "a ***one-time application token*** which includes assertions about the running target application" that is "a globally unique ***time-locked one-time application token***." (Starnes, paragraphs [0017], [0029], [0032] and [0039] (emphasis added)). Starnes describes that "the trust broker service issues an application token, which can be digitally-signed, and which includes the globally unique identifier of the application instance together with weighted trust scores assigned to that application instance on that machine." (Starnes, paragraph [0020]). Thus, Starnes' application tokens are <u>one-time time-locked</u> tokens that include trust scores <u>for a specific application instance on a</u> given <u>machine</u>. Nowhere does Starnes expressly or inherently disclose that the trust broker is capable of generating "a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application," as recited in claim 1.

With reference to FIG. 1, Starnes discloses that a "trust monitor service 120 detects and tracks the start and termination of applications on the operating system 105 platform . . . [t]he running application's property value assertions (PVAs) are measured at runtime and reported over a secure communications channel to a trust broker service 130 . . . [t]he trust broker service 130 requests a verification report for the running application on the target machine 100 and target platform 105" and the "trust broker service 130 generates and returns an application token 150 for the

running application." (Starnes, paragraph [0023]). Thus, as discussed during the interview, the one-time, time-locked application tokens generated by Starnes' trust broker are generated at a point in time when an application starts or terminates on a specific target machine or operating system platform. Similarly, Starnes' verification report is limited to an application running on a specific target machine or platform.

Starnes does not disclose "a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components," as recited in claim 1. Starnes describes that a "trust broker service 130 requests a verification report for the running application on the target machine 100 and target platform 105" and a "trust evaluation server may perform a real time measurement and verification of the target application or ***lookup the most recent verification test results based on a*** continuous ***monitoring schedule*** and return the verification report to the requestor." (Starnes, paragraph [0023] (emphasis added)). Starnes discloses that a "weighted trust score is a category based rating of level of concern" and "ratings are determined by factors that may include verification results, date and time of last verification scans." (Starnes, paragraph [0020]). Starnes further discloses that the trust broker service verifies the authenticity of the running application on the target device "with a ***near real time*** exchange of the metadata" with a trust evaluation server "and records of ***most recent*** measurements and ***verifications on the target device***." (Starnes, paragraphs [0028], [0032] and [0038] (emphasis added)). Thus, at best, Starnes' application verification is based on a lookup of recorded past, albeit "most recent", test results and verifications based on a "near real time exchange" of metadata or the scheduled verification scans that

occurred at a past "date and time." Aside from the above-quoted passages, Starnes lacks any disclosure or description of the "verification report", "real time measurement and verification", or the "verification test results." As such, it cannot be fairly concluded that Starnes' verification report is based on an execution analysis of executable file binaries and loaded components of the running application. Accordingly, Starnes fails to teach or suggest "wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components," as recited in claim 1.

Starnes is also silent regarding the capability of including a runtime execution context indicating executable file binaries and loaded components of the application in the alleged 'application tokens.' Instead, Starnes describes that a "trust evaluation server" monitors a "target device 400 based on a schedule to scan and verify the state of the running applications" based upon "binary hashes and properties of all application package components including dynamically loadable modules" against checklists. (Starnes, paragraph [0037]). As discussed during the interview, verifying an application state on a given device based upon comparing the results of a scheduled scan of binary hashes and loadable modules to a set checklist is not analogous to "attributes of the application at runtime comprising executable file binaries and loaded components of the application. As such, it cannot be fairly concluded that Starnes discloses, expressly or inherently, "a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application," as recited in claim 1.

Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejection of claim 1, and pass this claim to allowance.

Claims 2-12

At least based on their respective dependencies to claim 1, claims 2-12 should be found allowable, as well as in view of their additional distinguishing features. *See, In Re Fine*, 837 F.2d 1071 (Fed. Cir. 1988) and M.P.E.P. § 2143.03.

For example, claim 3 as amended herein recites, among other features, "wherein the attributes further comprise parent-child process associations of the application." As discussed above with regard to the application attributes recited in claim 1, Starnes does not disclose "a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application." The one-time, time-locked application tokens generated by Starnes' trust broker do not comprise any parent-child process associations of an application at runtime. As such, Starnes fails to disclose application attributes comprising "parent-child process associations of the application," as recited in claim 3.

Also, for example, claim 4 as amended herein recites, *inter alia*, "wherein the execution analysis is a static, dynamic, or virtual analysis of the one or more executable file binaries and the loaded components." As discussed above, Starnes' "verification report", "real time measurement and verification" and "verification test results" do not disclose security information comprising "an execution analysis of the one or more executable file binaries and the loaded components," as recited in claim 1. Starnes lacks any disclosure of an "execution analysis of the one or more executable file binaries and the loaded components" of an application, let alone an

execution analysis that "is a static, dynamic, or virtual analysis of the one or more executable file binaries and the loaded component," as recited in claim 4.

Applicants submit that claims 3 and 4 are further allowable over Starnes for at least these additional reasons.

Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejections of claims 2-12, and find these claims allowable over the applied reference.

Claim 13

At page 3 of the Office Action, the Office alleges that Starnes discloses all of the features of independent claim 13 in the Abstract and paragraphs [0028] - [0029] and [0038] – [0039]. Even assuming *arguendo* that the Office's interpretation of the above-noted portions of Starnes is correct, which Applicants do not concede, Starnes does not disclose regarding the above-quoted distinguishing features of claim 13.

With regard to previously-pending claim 13, the Office asserts that Starnes discloses "generating and sending application statements to the client and the server or the first and second peers about interrelated applications used in the client-server or peer-to-peer transactions" at paragraphs [0038] - [0039]. (Office Action, page 3). With reference to FIG. 4, paragraphs [0038] and [0039] of Starnes discuss "a runtime application profile (metadata), which comprises at least the file hash digests, and product instance specific property value assertions (PVAs) and resources" wherein a "trust broker service 470 verifies the authenticity of the running application on the target device 400 with ***a near real time*** exchange of the metadata 471 with a trust

evaluation server 410" and "generates a globally unique ***time-locked one-time application token*** 422 and returns the token to the trust monitor service 420."

As discussed during the personal interview, Applicants submit that a "near real time" exchange of metadata comprising file hash digests and PVAs and use of a "time-locked one-time" token does not teach or suggest the application artifact features recited in previously-pending claim 13. However, merely to expedite prosecution, Applicants have amended claim 13 as noted above to further clarify the recited application artifact. For example, claim 13 as amended herein recites, among other features, "generating and sending, by the attestation server, a first ***application artifact*** that ***dynamically and opaquely identifies***: ***an instance of a*** first ***application***; ***and a record of a current execution state of the*** first ***application***."

Support for these amendments is found at least, at for example, paragraphs [0008], [0019], [0025], [0033], [0036], [0047], [0060], [0067], [0083], [0090], [0092], [0094], [0097], [0115], [0127], [0132], [0137], [0141], [0147] and FIG. 12 of the instant specification. For example, the specification describes exemplary embodiments wherein "applications may be qualified based on . . . one or more attributes of the application (e.g., run time instance of the application) such as . . . an application fingerprint, (2) other applications/processes called by the application, (3) ports used by the application, (4) computing, storage, and network resource usage by the application . . . [s]uch information may be available . . . in the current execution context" and an "application 302 may include (for example, may embed, as a markup) the received application artifact 309 as an assertion (e.g., in a security assertion markup language (SAML or other common form of markup)) to the identity

provider 303 which may use back-channel communications 310 with the attestation broker 304 to verify the application artifact 309." (Applicants' specification, paragraphs [0025] and [0067]). Also, for example, paragraph [0090] of Applicants' specification provides:

> In certain exemplary embodiments, the client application 501 and the server application 501 may be statically or dynamically linked to the API library 516 (e.g., a Trust-as-a-Service (TAAS) API library). The API library 516 may implement a set of procedure calls for applications to exchange messages (e.g., opaque and/or secure messages) with an attestation service or broker 502 that may hide the implementation details from the higher level application.

Thus, the specification describes exemplary embodiments wherein opaque messaging can be used to exchange application artifacts and subsequent change notification can be facilitated via use of an application artifact as a callback mechanism.

Applicants submit that using a trust monitor service to monitor state changes of an application such as "configuration settings, active listening ports at the transport layer of the OSI stack, and terminations of the applications" and notifying a trust broker service "in near real time" so that it can store "persistent and transient state metadata in a local database or remote repository" (Starnes, paragraph [0039]) does not disclose generating, sending, and validating an application artifact that dynamically and opaquely identifies an instance of the application and a record of a current execution state of the application. Thus, Starnes does not expressly or inherently disclose "generating and sending by the attestation server, a first application artifact that dynamically and opaquely identifies: an instance of a first application; and a record of a current execution state of the first application" and "receiving and validating . . . the first application artifact sent by the attestation server

to a client in a client server transaction or to a second peer in the peer-to-peer transaction," as recited in claim 13.

Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejection of claim 13, and find this claim allowable over Starnes.

Claims 14-16

At least based on their respective dependencies to claim 13, claims 14-16 should be found allowable, as well as in view of their additional distinguishing features.

Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejections of claims 14-16, and find these claims allowable over the applied reference.

Claim 17

At pages 3-4 of the Office Action, the Office alleges that Starnes discloses all of the features of claim 17 in the Abstract and paragraphs [0019] - [0021] and [0033] – [0040]. Even assuming *arguendo* that the Office's interpretation of the above-noted portions of Starnes is correct, to which Applicants do not acquiesce, Starnes does not disclose regarding the above-quoted distinguishing features of claim 17.

With regard to previously-pending claim 17, the Office asserts that Starnes discloses "requesting an application artifact for a running web application or servlet instance" at paragraphs [0033] - [0034] and "generating at least one hash file digest corresponding to the execution context of the web application or servlet instance" and "determining at least one file attribute corresponding to at least one element or the execution context of the web application or web servlet instance" at paragraphs [0019] - [0021]). (Office Action, page 4).

Starnes describes a "collection of digests of files, data elements and properties . . . for the running target application on the target machine (or device)" reporting "these digests and properties in a digitally-signed integrity report" and "based on the digests and property value assertions (PVAs) in the integrity report, the trust evaluation servers can verify each digest and property, to the extent possible, against a signature and reference harvest database (part of the trust scoring system)." (Starnes, paragraph [0019]). Starnes further describes that "[a]s an outcome of the evaluation of the running target application ***on the target machine by the trust scoring system***, the trust broker service issues an application token, which can be digitally-signed, and ***which includes*** the globally unique identifier of the application instance together with ***weighted trust scores assigned to that application*** instance ***on that machine***" and "[t]he application token may be used by web browsers (i.e. passive clients)." (Starnes, paragraphs [0020] and [0021] (emphasis added)). With reference to FIG. 3, Starnes describes that a "web application 340 includes (for example, embeds) the received application token as an assertion," the application token is then verified and validated and a "trust broker service 370" determines "whether logical access to the resource (the web application instance), based on an authorization profile configured for the trust broker service 370, should be granted for the user to access the web application." (Starnes, paragraphs [0033] and [0034]).

As discussed during the aforementioned interview, Applicants submit that a use of a digitally-signed integrity report and an application token including weighted trust scores assigned to a web application on a particular machine by a web browser to determine whether or not to grant user access to the web application does not

teach or suggest the application artifact and file attribute features recited in previously-pending claim 17. However, as noted above, merely to expedite prosecution, Applicants have amended claim 17 to further clarify the recited application artifact and execution context. For example, claim 17 recites, *inter alia*:

> requesting ***an application artifact that is a dynamic, opaque reference to a running*** web ***application or*** servlet ***instance***;
>
> . . .
>
> generating at least one ***digital signature corresponding to the execution context*** of the web application or servlet instance; [and]
>
> determining at least one ***parent-child process association corresponding to the execution context***.

By way of example and not limitation, Applicants' specification describes that runtime application and client application contexts can include "file attributes of components" of a running server or client application "including parent-child process associations and loader dependencies." (Applicants' specification, paragraphs [0038], [0058], [0092] and [0094]). Starnes discloses a "digitally-signed integrity report" and verifying "digests and property value assertions (PVAs) in the integrity report . . . against a signature and reference harvest database" that is part of a "trust scoring system." (Starnes, paragraph [0019]). However, nowhere does Starnes disclose "an application artifact that is a dynamic, opaque reference to a running web application or servlet instance," generating a "digital signature corresponding to the execution context of the web application or servlet instance," or determining a "parent-child process association corresponding to the execution context," as recited in claim 17. As such, Starnes does not anticipate independent claim 17.

Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejection of claim 17, and find this claim allowable over the applied reference.

Claims 18-20

At least based on their dependencies from independent claim 17, claims 18-20 should be found allowable, as well as in view of their additional distinguishing features.

Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejections of claims 18-20, and pass these claims to allowance.

Claim 21

At pages 4-6 of the Office Action, the Office alleges that Starnes discloses all of the features of independent claim 22 in the Abstract and paragraphs [0007] - [0010], [0020], [0025] - [0029], [0031] - [0034], [0037], and [0039]. Even assuming for the sake of argument that the Office's interpretation of the above-noted portions of Starnes is correct, which Applicants do not concede, Starnes does not disclose regarding the above-quoted distinguishing features of claim 22.

As noted in the Examiner's interview summary, during the interview the Examiner "agreed that Starnes does not teach 'remediating' on the cited section." Applicants agree and further note that "remediating the instrumented target platform, wherein the remediating includes one or more of: a reimage, a snapshot, or a quarantine of the instrumented target platform," as recited in claim 21 is not disclosed in the cited portion of Starnes (e.g., paragraph [0037]) or any other portion. In fact, Starnes is silent regarding any of the above-noted remediating elements of reimaging, taking a snapshot, or quarantining a platform.

As was clarified during the interview, the reference to "par.20" at page 5 of the Office Action as allegedly disclosing "continuously display the dynamic assertions to a system administrator" is a typographical error and the Examiner meant to state

"par.21." Starnes describes that a web browser "can display an ***application trust attestation logo*** at the bottom of the web page ***displayed to the user*** to provide attestation of application authenticity and trustworthiness . . . ***[t]he user that clicks that*** application trust attestation ***logo*** is shown application instance specific trust score" that was "issued (digitally-signed) by the trust broker service for that given target web application" based upon an application token "used . . . to determine ***near real-time information*** about the state of a running application ***on a target machine***." (Starnes, paragraph [0021] (emphasis added)). As discussed during the interview, Applicants submit that Starnes' trust attestation logo that can be selected by a specific user to show a "specific trust score" for an application based on near-real time information about the application on a specific target machine does not disclose a "a graphical user interface configured to: ***request and receive dynamic assertions***. . . pertaining to the local execution context or the introspected security context of running application instances" and "***continuously display the dynamic assertions***," as recited in claim 21.

With regard to previously-pending claim 21, the Office alleges paragraph [0039] of Starnes teaches "generating a globally unique, opaque, and time-sensitive application artifact and application statements including a plurality of assertions pertaining to inspection based runtime local execution context and introspection based security context." As noted above, without acquiescing to the propriety of any rejection, Applicants have amended claim 21 to clarify the recited application artifact. For example, amended claim 21 recites, among other features, "generating globally unique, opaque, and time-sensitive application ***artifacts identifying records of current execution states*** and application statements ***for the target, running***

applications including a plurality of assertions pertaining to inspection based runtime local execution context and introspection based security context."

Starnes describes that the trust broker service "generates a globally unique ***time-locked one-time application token***", a trust monitor service "***monitors*** the running applications instances for ***state changes***, including . . . ***configuration settings***, active listening ports at the transport layer of the OSI stack, and ***terminations of the applications***" and the trust broker service "***stores persistent*** and transient ***state metadata*** in a local database or remote repository . . . ***for all registered*** running ***applications*** instances ***on the target device***." (Starnes, paragraph [0039] (emphasis added)). As discussed during the aforementioned interview, Applicants submit that using time-locked one time application tokens, monitoring application state changes such as configuration settings and terminations and storing persistent state metadata for registered applications on a specific target device is not analogous to "generating globally unique, opaque, and time-sensitive application ***artifacts identifying records of current execution states*** and application statements ***for the target, running applications***," as recited in claim 21.

Claim 21 also recites "discovering, identifying and inspecting running application processes on the instrumented target platform, wherein the discovering includes analysis of executable file binaries of the target, running applications." Starnes is silent regarding the capability of discovering applications through analysis of executable file binaries of running applications. In contrast, the application discovery recited in claim 21 is performed through analyzing an executing binary of a currently-running application.

Thus, Starnes fails to expressly or inherently disclose at least the above-noted distinguishing features of claim 21.

Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejection of claim 21 and find this claim allowable over Starnes.

Claims 22-26

At least based on their dependencies from claim 21, claims 22-26 should be found allowable, as well as in view of their additional distinguishing features.

Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejections of claims 22-26, find these claims allowable over the applied reference.

CONCLUSION

All of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicants therefore respectfully request that the Examiner reconsider all presently outstanding rejections and that they be withdrawn. Applicants believe that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: 29 June 2012

By: / R. K. Baldwin /
Randall K. Baldwin
Attorney for Applicants
Registration No. 59,713

Customer No. 21839
703 836 6620

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	**MAIL STOP AMENDMENT**
Kumar, Srinivas et al.	Group Art Unit: 2436
Application No.: 13/399,065	Examiner: Cervetti, David Garcia
Filed: February 17, 2012	Confirmation No.: 3713
For: System and Method for Application Attestation	

FIRST INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure as set forth in 37 C.F.R. § 1.56, the accompanying information is being submitted in accordance with 37 C.F.R. §§ 1.97 and 1.98.

In accordance with 37 C.F.R. § 1.98(a)(2), copies of the listed U.S. patent application publications cited on the attached IDS Form are not submitted.

The documents are being submitted after a first Office Action on the merits but prior to the closing of prosecution, therefore under 37 C.F.R. § 1.97(c), the fee set forth in 37 C.F.R. § 1.17(p) is enclosed.

A fee of $180.00 (1806) as set forth in 37 C.F.R. § 1.17(p) is enclosed.

To assist the Examiner, the documents are listed on the attached form PTO/SB/O8. It is respectfully requested that an Examiner-initialed copy of this form be returned to the undersigned.

The Director is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17 and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: 29 June 2012

By: / R. K. Baldwin /
Randall K. Baldwin
Registration No. 59,713

Customer No. 21839
703 836 6620

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	1	of	1

Complete if Known	
Application Number	**13/399,065**
Filing Date	**February 17, 2012**
First Named Inventor	**Kumar, Srinivas**
Art Unit	**2436**
Examiner Name	**Cervetti, David Garcia**
Attorney Docket Number	**0079152-000002**

U.S. PATENT DOCUMENTS

Examiner Initials'	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2009/0144818	A1	06-04-2009	Kumar *et al.*.	
		US-2009/0138939	A1	05-28-2009	Kumar *et al.*	
		US-2009/0276204	A1	11-05-2009	Kumar *et al.*	
		US-2009/0241170	A1	09-24-2009	Kumar *et al.*	
		US-2009/0133110	A1	05-21-2009	Kumar *et al.*	
		US-2009/0328186	A1	12-31-2009	Pollutro *et al.*	

FOREIGN PATENT DOCUMENTS

Examiner Initials'	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional). 2 See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. 3 Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). 4 For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. 5 Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. 6 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Patent Application Fee Transmittal

Application Number:	13399065
Filing Date:	17-Feb-2012
Title of Invention:	SYSTEM AND METHOD FOR APPLICATION ATTESTATION
First Named Inventor/Applicant Name:	Srinivas KUMAR
Filer:	Randall K. Baldwin/Ritsuko Dale
Attorney Docket Number:	0079152-000002

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt

EFS ID:	13146423
Application Number:	13399065
International Application Number:	
Confirmation Number:	3713
Title of Invention:	SYSTEM AND METHOD FOR APPLICATION ATTESTATION
First Named Inventor/Applicant Name:	Srinivas KUMAR
Customer Number:	21839
Filer:	Randall K. Baldwin/Ritsuko Dale
Filer Authorized By:	Randall K. Baldwin
Attorney Docket Number:	0079152-000002
Receipt Date:	29-JUN-2012
Filing Date:	17-FEB-2012
Time Stamp:	15:45:24
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$180
RAM confirmation Number	3116
Deposit Account	024800
Authorized User	BALDWIN,RANDY

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		13-399065_AMDT_04-27-12-OA.pdf	1438647 a371472708cbe4cecb1dc8a766e033073f4051e7	yes	35
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Amendment/Req. Reconsideration-After Non-Final Reject		1	1	
	Specification		2	3	
	Claims		4	14	
	Applicant Arguments/Remarks Made in an Amendment		15	35	
Warnings:					
Information:					
2		13-399065_IDS-SBO8.pdf	126831 2bd4721a46581f5f149214ee44b8f1b20170ef2e	yes	3
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Transmittal Letter		1	2	
	Information Disclosure Statement (IDS) Form (SB08)		3	3	
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30480 7f145e98b67aea20112b745e9780782bf310d087	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1595958		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
13/399,065	02/17/2012	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 06/29/2012	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 26	Minus	** 26	= 0	X $30 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $125 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/SUSAN FORD/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/399,065	02/17/2012	Srinivas KUMAR	0079152-000002	3713

21839 7590 06/14/2012
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER
CERVETTI, DAVID GARCIA

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
06/14/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com
offserv@bipc.com

Trend Micro, Inc.
EX1002-106

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	13/399,065	KUMAR ET AL.	
	Examiner	Art Unit	
	David García Cervetti	2436	

All participants (applicant, applicant's representative, PTO personnel):

(1) *David García Cervetti*.

(2) *Chad Wieland*.

(3) *Randall K. Baldwin (Reg.No.59,713)*.

(4) *Srinivas Kumar*.

Date of Interview: *07 June 2012*.

Type: ☐ Telephonic ☐ Video Conference
☒ Personal [copy given to: ☒ applicant ☒ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☐ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☒102 ☐103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1,13,17 and 21*.

Identification of prior art discussed: *Starnes (2011/0179477)*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

The claims were discussed, the rejection of claim 21, step of remediating, was discussed. It was agreed that Starnes does not teach "remediating" on the cited section. Possible amendment including a definition of what attributes and artifacts/statements are as opposed to Starnes' application token, and how they differentiate over Starnes.

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/David García Cervetti/ Primary Examiner, Art Unit 2436	

Trend Micro, Inc.
EX1002-107

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/399,065	02/17/2012	Srinivas KUMAR	0079152-000002	3713

21839 7590 04/27/2012
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER
CERVETTI, DAVID GARCIA

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
04/27/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com
offserv@bipc.com

Trend Micro, Inc.
EX1002-109

Office Action Summary	Application No.	Applicant(s)	
	13/399,065	KUMAR ET AL.	
	Examiner	Art Unit	
	David García Cervetti	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 February 2012*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-26* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-26* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *17 February 2012* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

Trend Micro, Inc.
EX1002-110

DETAILED ACTION

1. Claims 1-26 are pending and have been examined.

Information Disclosure Statement

2. It is noted that no Information Disclosure Statement has been filed.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. The following claims are rejected under 35 U.S.C. 102(e) as being anticipated by Starnes (20110179477).

Regarding claim 1, Starnes teaches

A method of providing an attestation service for an application at runtime executing on a computing platform using an attestation server (abstract), comprising:

receiving, by the attestation server remote from the computing platform:

a runtime execution context indicating attributes of the application at runtime (par.17); and

a security context providing security information about the application (par.23);

generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result (par.28-29); and

sending, by the attestation server, the attestation result associated with the application (par.28-29).

Regarding claim 13, Starnes teaches

A non-transitory computer readable medium having instructions stored thereon that, if executed by a computing device, cause the computing device to perform operations for providing mutual attestation of applications in client-server or peer-to-peer transactions using an attestation server (abstract), the operations comprising:

generating and sending, by the attestation server, a first application artifact (par.28-29);

receiving and validating, by the attestation server from a server in the client server transaction or from a first peer in the peer-to-peer transaction, the first application artifact sent by the attestation server to a client in a client server transaction or to a second peer in the peer-to-peer transaction (par.38-39);

generating and sending application statements to the client and the server or the first and second peers about interrelated applications used in the client-server or peer-to-peer transactions (par.38-39).

Regarding claim 17, Starnes teaches

A method for providing attestation of the authenticity of a running web application or web servlet using an attestation server (abstract), comprising:

requesting an application artifact for a running web application or servlet instance (par.33-34);

establishing a secure channel between the web server and the attestation server (par.33-34);

generating at least one hash file digest corresponding to the execution context of the web application or servlet instance (par.19-21);

determining at least one file attribute corresponding to at least one element or the execution context of the web application or web servlet instance (par.19-21);

sending an application report to an identity provider (par.34-37);

generating assertions based on a received security context and a received local execution context (par.39-40);

transmitting confidence metrics in the report to the identity provider (par.37-39); and

providing attestation of the running web application or web servlet as a digital icon for rendering by a web browser (par.33).

Regarding claim 21, Starnes teaches

A system for continuously monitoring running applications hosted on self-managed and on-premise, or on outsourced service provider managed infrastructure comprising (abstract):

an instrumented target platform for hosting a target user or service program (par.10);

an application attestation service for: generating a globally unique, opaque, and time-sensitive application artifact and application statements including a plurality of assertions pertaining to inspection based runtime local execution context and introspection based security context (par.39); and

remediating the instrumented target platform, wherein the remediating includes one or more of: a reimage, a snapshot, or a quarantine of the instrumented target platform (par.37);

a runtime monitor for discovering, identifying and inspecting running application processes on the instrumented target platform and for generating metadata that includes at least the runtime local execution context (par.27-29);

a collaboration service configured to:

provide introspected security context for a target application running on the instrumented target platform (par.7-10); and

analyze executable file binaries for the target application running on the instrumented target platform (par.31-32); and

a graphical user interface configured to:

request and receive dynamic assertions from a metadata repository of the attestation service, the dynamic assertions pertaining to the local execution context the introspected security context of running application instances on instrumented target platforms (par.32-34);

continuously display the dynamic assertions to a system administrator (par.20); and

provision and dispatch alerts based on the dynamic assertions and predefined criteria (par.25-29).

Regarding claim 2, Starnes teaches generating, by the attestation server, an application artifact as a reference for changes in a subsequent execution context (par.39-40); and sending the generated application artifact such that subsequent changes to the runtime execution context are tracked based on the generated application artifact (par.39-40).

Regarding claim 3, Starnes teaches digitally signing the attestation results and the application artifact (par.9 and 20).

Regarding claim 4, Starnes teaches wherein the received security context is an introspective security context (par.7-10).

Regarding claim 5, Starnes teaches wherein the generating of the report indicating security risks associated with the application includes generating, by the attestation server, one or more security assertions that pertain to the received runtime execution context and the received introspective security context (par.25-26).

Regarding claim 6, Starnes teaches authenticating the application using a plurality of collaboration services (par.19-21).

Regarding claim 7, Starnes teaches controlling a user's transaction with the application by applying a set of authorization rules in accordance with the attestation results (par.33-34).

Regarding claim 8, Starnes teaches controlling a user's network access to the application by applying a set of authorization rules in accordance with the attestation results (par.33-34).

Regarding claim 9, Starnes teaches providing confidence metrics in the attestation results indicating a level of security risk by different classifications such that a restriction on a user's transaction with the application are applied based on the level of security risk indicated by the confidence metrics in the attestation results (par.29-30).

Regarding claim 10, Starnes teaches wherein the application of the restriction on the user's transaction includes applying the restriction on the user's network access to the application (par.33-34).

Regarding claim 11, Starnes teaches wherein the application of the restriction on the user's transaction includes applying routing decisions and redirecting the user to an alternate computer platform (par.25-26).

Regarding claim 12, Starnes teaches controlling, by a network access enforcer, access of a user to the application based on the attestation result (par.25-26).

Regarding claim 14, Starnes teaches generating and sending, by the attestation server, a second application artifact; receiving and validating, by the attestation server from a client in the client server transaction or from a second peer in the peer-to-peer transaction, the second application artifact sent by the attestation server to a server in a client server transaction or to a first peer in the peer-to-peer transaction (par.27-29).

Regarding claim 15, Starnes teaches the sending of the application statements to the client and the server or the first and second peers comprises the following

operations: sending by the attestation server: the application statement regarding a client application of the interrelated applications to the server of the client-server transaction and the application statement regarding a server application of the interrelated applications to the client of the client-server transaction; or the application statement regarding a first peer application of the interrelated applications to the second peer of the peer-to-peer transaction and the application statement regarding a second peer application of the interrelated applications to the first peer of the peer-to-peer transaction (par.27-29); and determining, based at least in part upon the sent application statements, whether to transact data exchanges with associated applications (par.30-35).

Regarding claim 16, Starnes teaches the generating of the application statements includes: including in the application statements confidence metrics and contextual assertions (par.28-29); and the determining whether to transact data exchanges with the associated applications includes: comparing respective confidence metrics to a set of rules; and determining whether to transact data exchange based on the comparison (par.33-35).

Regarding claim 18, Starnes teaches wherein the attestation is provided prior to commencing any data exchange in an established connection with a user (par.17-19).

Regarding claim 19, Starnes teaches wherein the attestation is provided prior to establishing a network connection with a user (par.17-19).

Regarding claim 20, Starnes teaches rendering attestation information about the web application to be accessed responsive to user input (par.33-34).

Regarding claim 22, Starnes teaches wherein a network access enforcer subscribes for and receives dynamic application statements from an attestation service to analyze the contextual assertions and determine whether an authenticated user is permitted or denied network access to an attested application instance (par.25).

Regarding claim 23, Starnes teaches wherein the graphical user interface displays the applications running on instrumented target platform on a client specific dashboard or portal, and presents for each associated application execution context at least one of: a service hostname; a service realm; a service principal name; a product version; a product vendor; one or more classifications based confidence metrics; an active network service port; or executable file binaries (par.27-29).

Regarding claim 24, Starnes teaches an identity provider that queries for dynamic application statements from the attestation server to analyze the contextual assertions and to determine whether an authenticated user is permitted or denied authorization to transact data exchanges with an attested application instance in an established connection (par.34-39).

Regarding claim 25, Starnes teaches a network access enforcer that analyzes classifications based confidence metrics included in received dynamic application statements, based on a subscription, from an attestation service to determine whether an authenticated user is permitted or denied network access to an attested application instance (par.25-27).

Regarding claim 26, Starnes teaches wherein an identity provider analyzes classifications based confidence metrics included in received dynamic application

statements, based on a subscription, from an attestation service to determine whether an authenticated user is permitted or denied authorization to transact data exchanges with an attested application instance in an established connection (par.34-39).

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David García Cervetti whose telephone number is (571)272-5861. The examiner can normally be reached on Monday-Friday 8 AM to 5 PM.
6. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Philip J. Chea can be reached on (571)272-3951. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.
7. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/David García Cervetti/
Primary Examiner, Art Unit 2436

Notice of References Cited	Application/Control No. 13/399,065	Applicant(s)/Patent Under Reexamination KUMAR ET AL.	
	Examiner David García Cervetti	Art Unit 2436	Page 1 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2005/0033987 A1	02-2005	Yan et al.	713/201
*	B	US-2005/0132202 A1	06-2005	Dillaway et al.	713/179
*	C	US-2005/0132031 A1	06-2005	Sailer et al.	709/223
*	D	US-2005/0138384 A1	06-2005	Brickell et al.	713/182
*	E	US-2005/0221766 A1	10-2005	Brizek et al.	455/073
*	F	US-2006/0005009 A1	01-2006	Ball et al.	713/155
*	G	US-7,194,759 B1	03-2007	Chess et al.	726/2
*	H	US-2007/0185856 A1	08-2007	Mittal et al.	707/005
*	I	US-2008/0015808 A1	01-2008	Wilson et al.	702/123
*	J	US-2008/0083039 A1	04-2008	CHOI et al.	726/27
*	K	US-2008/0141027 A1	06-2008	Kim et al.	713/156
*	L	US-2008/0235372 A1	09-2008	Sailer et al.	709/224
*	M	US-2008/0289028 A1	11-2008	Jansen et al.	726/11

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Trend Micro, Inc.
EX1002-120

Notice of References Cited	Application/Control No. 13/399,065	Applicant(s)/Patent Under Reexamination KUMAR ET AL.	
	Examiner David García Cervetti	Art Unit 2436	Page 2 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2009/0178138 A1	07-2009	Weiss et al.	726/22
*	B	US-2009/0204964 A1	08-2009	Foley et al.	718/1
*	C	US-2009/0204806 A1	08-2009	Kanemura et al.	713/155
*	D	US-7,587,607 B2	09-2009	Brickell et al.	713/182
*	E	US-7,797,544 B2	09-2010	Dillaway et al.	713/179
*	F	US-2010/0281273 A1	11-2010	Lee et al.	713/190
*	G	US-7,882,221 B2	02-2011	Sailer et al.	709/224
*	H	US-2011/0035577 A1	02-2011	Lin et al.	713/150
*	I	US-2011/0154500 A1	06-2011	Sahita et al.	726/26
*	J	US-7,979,696 B2	07-2011	Kim et al.	713/156
*	K	US-2011/0173643 A1	07-2011	Nicolson et al.	719/328
*	L	US-2011/0179477 A1	07-2011	Starnes et al.	726/9
*	M	US-8,108,536 B1	01-2012	Hernacki et al.	709/231

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Trend Micro, Inc.
EX1002-121

Notice of References Cited	Application/Control No. 13/399,065	Applicant(s)/Patent Under Reexamination KUMAR ET AL.	
	Examiner David García Cervetti	Art Unit 2436	Page 3 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2012/0084850 A1	04-2012	Novak et al.	726/8
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Trend Micro, Inc.
EX1002-122

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13399065	KUMAR ET AL.
	Examiner	**Art Unit**
	David García Cervetti	2436

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/11/2012								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								
	26	✓								

Trend Micro, Inc.
EX1002-123

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 3713

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/399,065	02/17/2012 **RULE**	726	2436	0079152-000002

APPLICANTS
Srinivas KUMAR, Cupertino, CA;
Gurudatt Shashikumar, Foster City, CA;

**** CONTINUING DATA ***************************
This appln claims benefit of 61/443,854 02/17/2011

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
03/01/2012

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☑ Yes ☐ No Verified and Acknowledged /DAVID GARCIA CERVETTI/ Examiner's Signature	☐ Met after Allowance DGC Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CA	11	26	4

ADDRESS
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404
UNITED STATES

TITLE
SYSTEM AND METHOD FOR APPLICATION ATTESTATION

FILING FEE RECEIVED		
1135	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13399065	KUMAR ET AL.
	Examiner	**Art Unit**
	David García Cervetti	2436

SEARCHED

Class	Subclass	Date	Examiner
726	22,23,24,25	4/11/2012	DGC

SEARCH NOTES

Search Notes	Date	Examiner
inventor name search, acm, ieee, springer, google, scholar, east history attached	4/11/2012	DGC

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

	/David García Cervetti/ Primary Examiner.Art Unit 2436

Trend Micro, Inc.
EX1002-125

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L4	20	(application program) near5 attest$ near8 server	US-PGPUB; USPAT	OR	OFF	2012/04/13 08:49
L5	13	(application program) near5 (correct$ remediat$) and attest$ near8 server	US-PGPUB; USPAT	OR	OFF	2012/04/13 09:34
L6	18	(application program) near5 (update updating reimage snapshot correct$ remediat$) and attest$ near8 server	US-PGPUB; USPAT	OR	OFF	2012/04/13 09:37
L7	48	(application program) near5 (update updating reimage snapshot correct$ remediat$) and attest$ near8 (application program)	US-PGPUB; USPAT	OR	OFF	2012/04/13 09:38
S1	3286	726/22.ccls.	US-PGPUB; USPAT	OR	OFF	2012/04/11 23:30
S2	2280	726/23.ccls.	US-PGPUB; USPAT	OR	OFF	2012/04/11 23:30
S3	1855	726/24.ccls.	US-PGPUB; USPAT	OR	OFF	2012/04/11 23:30
S4	1422	726/25.ccls.	US-PGPUB; USPAT	OR	OFF	2012/04/11 23:30
S5	167	(runtime execution executing) near7 (attest$)	US-PGPUB; USPAT	OR	OFF	2012/04/11 23:39
S6	20	(runtime execution executing) near7 (attest$) near8 server	US-PGPUB; USPAT	OR	OFF	2012/04/11 23:39
S7	62	(runtime execution executing) near5 (application context program) and (attest$) near8 server	US-PGPUB; USPAT	OR	OFF	2012/04/11 23:42
S8	1	"7540030".pn.	US-PGPUB; USPAT	OR	OFF	2012/04/12 09:22
S9	1	"20030212906".pn.	US-PGPUB; USPAT	OR	OFF	2012/04/12 09:22
S10	1	"7540030".pn. and (log logfile record)	US-PGPUB; USPAT	OR	OFF	2012/04/12 09:24
S11	1	"20030212906".pn. and (log logfile record)	US-PGPUB; USPAT	OR	OFF	2012/04/12 09:25
S12	38	(application program) near5 attest$ and (attest$) near8 server	US-PGPUB;	OR	OFF	2012/04/12 14:47

USPAT

EAST Search History (Interference)

<This search history is empty>

4/13/2012 10:29:41 AM
H:\Workspaces\Workspaces\13-399-065-04-11-2012.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/399,065	02/17/2012	Srinivas KUMAR	0079152-000002	3713

21839 7590 03/29/2012
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER
CHEA, PHILIP J

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
03/29/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com
offserv@bipc.com

Doc Code: TRACK1.GRANT

Decision Granting Request for Prioritized Examination (Track I or After RCE)	Application No.:13/399065

1. THE REQUEST FILED 02/17/12 IS **GRANTED**.

   The above-identified application has met the requirements for prioritized examination
   A. ☒ for an original nonprovisional application (Track I).
   B. ☐ for an application undergoing continued examination (RCE).

2. **The above-identified application will undergo prioritized examination.** The application will be accorded special status throughout its entire course of prosecution until one of the following occurs:

   A. filing a **petition for extension of time** to extend the time period for filing a reply;
   B. filing an **amendment to amend the application to contain more than four independent claims, more than thirty total claims**, or a multiple dependent claim;
   C. filing a **request for continued examination**;
   D. filing a notice of appeal;
   E. filing a request for suspension of action;
   F. mailing of a notice of allowance;
   G. mailing of a final Office action;
   H. completion of examination as defined in 37 CFR 41.102; or
   I. abandonment of the application.

Telephone inquiries with regard to this decision should be directed to Tod Swann at 571-272-3612. In his/her absence, calls may be directed to Nasser Goodarzi, 571-272-4195.

/Tod Swann/
[*Signature*]

MQAS
(Title)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/399,065	02/17/2012	Srinivas KUMAR	0079152-000002

CONFIRMATION NO. 3713

POA ACCEPTANCE LETTER

21839
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

OC000000052924775

Date Mailed: 03/06/2012

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/17/2012.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/bpham/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Trend Micro, Inc.
EX1002-130

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/399,065	02/17/2012	2431	1135	0079152-000002	26	4

CONFIRMATION NO. 3713

21839
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

FILING RECEIPT

OC000000052924725

Date Mailed: 03/06/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Srinivas KUMAR, Cupertino, CA;
Gurudatt Shashikumar, Foster City, CA;

Assignment For Published Patent Application

TAASERA, INC., Erie, PA

Power of Attorney: The patent practitioners associated with Customer Number 21839

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/443,854 02/17/2011

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

Permission to Access - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

If Required, Foreign Filing License Granted: 03/01/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/399,065**

Projected Publication Date: 08/23/2012

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****

Trend Micro, Inc.
EX1002-131

Title

SYSTEM AND METHOD FOR APPLICATION ATTESTATION

Preliminary Class

726

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

Trend Micro, Inc.
EX1002-132

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number
13/399,065

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	95		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	310		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	125		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	26 minus 20 =	* 6	x 30 =	180	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	4 minus 3 =	* 1	x 125 =	125			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	835		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
AMENDMENT A	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
AMENDMENT A	Application Size Fee (37 CFR 1.16(s))									
AMENDMENT A	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
AMENDMENT B	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
AMENDMENT B	Application Size Fee (37 CFR 1.16(s))									
AMENDMENT B	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

☒ The filing fee has been calculated as follows:

☐ and in accordance with the enclosed Preliminary Amendment:

					FEES
Basic Patent Application Filing Fee (electronic filing for small entity) (4011)					$95.00
Examination Fee (2311)					$125.00
Search Fee (2111)					$310.00
	No. of Claims		Extra Claims	Rate	
Total Claims	26	Minus 20=	6	x $ 30.00 (2202)	180.00
Independent Claims	4	Minus 3=	1	x $ 125.00 (2201)	125.00
If multiple dependent claims are presented, add $225.00 (2203)					
App. Size Fee (app + dwgs. exceeding 100 sheets) - $155.00 / each add'l. 50 sheets (2081)					
TOTAL APPLICATION FEE DUE					**$835.00**

☒ Charge $835.00 to credit card. Filing fee is being paid electronically concurrent with filing of application.

☒ The Director is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17 and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800.

Please address all correspondence concerning this application to:

Buchanan Ingersoll & Rooney PC
Customer Number **2 1 8 3 9**

Respectfully submitted,

BUCHANAN-INGERSOLL & ROONEY PC

Date: February 17, 2012

By: _____
Charles F. Wieland III
Registration No. 33,096

Customer Number 21839
703.836.6620

03/02/2012 CCETIN 00000004 024800 13399065

01 FC:2201 125.00 DA
02 FC:2202 180.00 DA

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

UTILITY PATENT APPLICATION TRANSMITTAL LETTER FOR ELECTRONICALLY FILED UTILITY APPLICATION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Customer Number **2 1 8 3 9**

Sir:

Enclosed for filing is the utility patent application entitled:

SYSTEM AND METHOD FOR APPLICATION ATTESTATION

by the following named inventor(s):

Srinivas KUMAR; and Gurudatt SHASHIKUMAR

☒ Applicant(s) requests that the published application include the following assignment information: TAASERA, INC., Erie, Pennsylvania, USA.

☒ Small entity status is claimed.

Also enclosed are:

DRAWINGS: 11 sheets of drawings

DECLARATION: ☐ will follow ☒ executed, is enclosed ☐ unexecuted, is enclosed

ASSIGNMENT: ☐ is being filed electronically concurrent with the electronic filing of the application.
☐ will follow.

CLAIM FOR PRIORITY UNDER 35 USC § 119 and/or 365: ☐ is made in the declaration ☐ is hereby made as follows:

Country	Appl. No.	Filing Date MM-DD-YYYY

OTHER PAPERS:
☒ A General Authorization for Petitions for Extensions of Time and Payment of Fees
☒ An Application Data Sheet
☒ Other: Certification and Request for Prioritized Examination Under 37 CFR 1.102(e) (PTO/SB/424); Power of Attorney (PTO/SB/80); and Statement Under 37 CFR 3.73(b) (with copy of executed Assignment)

☒ The filing fee has been calculated as follows:

☐ and in accordance with the enclosed Preliminary Amendment:

					FEES
Basic Patent Application Filing Fee (electronic filing for small entity) (4011)					**$95.00**
Examination Fee (2311)					**$125.00**
Search Fee (2111)					**$310.00**
	No. of Claims		**Extra Claims**	**Rate**	
Total Claims	26	Minus 20=	6	x $ 30.00 (2202)	180.00
Independent Claims	4	Minus 3=	1	x $ 125.00 (2201)	125.00
If multiple dependent claims are presented, add $225.00 (2203)					
App. Size Fee (app + dwgs. exceeding 100 sheets) - $155.00 / each add'l. 50 sheets (2081)					
TOTAL APPLICATION FEE DUE					**$835.00**

☒ Charge $835.00 to credit card. Filing fee is being paid electronically concurrent with filing of application.

☒ The Director is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17 and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800.

Please address all correspondence concerning this application to:

Buchanan Ingersoll & Rooney PC
Customer Number **2 1 8 3 9**

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: February 17, 2012

By: _____
Charles F. Wieland III
Registration No. 33,096

Customer Number 21839
703.836.6620

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	
	)	
Srinivas KUMAR et al.	)	Group Art Unit: Unassigned
	)	
Application No.: Unassigned	)	Confirmation No.: Unassigned
	)	
Filed: February 17, 2012	)	
	)	
For: SYSTEM AND METHOD FOR APPLICATION ATTESTATION	)	
	)	
	)	
	)	

GENERAL AUTHORIZATION FOR PETITIONS FOR EXTENSIONS OF TIME AND PAYMENT OF FEES

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with 37 C.F.R. § 1.136(a)(3), the U.S. Patent and Trademark Office is hereby provided with a general authorization to treat any concurrent or future reply requiring a petition for an extension of time for its timely submission as containing a request therefor for the appropriate length of time.

The Commissioner is hereby authorized to charge any appropriate fees that may be required by this paper, or any other submissions in this application, and to credit any overpayment, to Deposit Account No. 02-4800.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: February 17, 2012

By: _____
Charles F. Wieland III
Registration No. 33,096

Customer Number 21839
703.836.6620

APPLICATION DATA SHEET

Application Information

Application Number::	
Filing Date::	
Application Type::	Nonprovisional
Subject Matter::	Utility
CD-ROM or CD-R?::	None
Computer Readable Form (CRF)?::	No
Title::	SYSTEM AND METHOD FOR APPLICATION ATTESTATION
Attorney Docket Number::	0079152-000002
Request for Early Publication?::	No
Request for Non-Publication?::	No
Total Drawing Sheets::	11
Small Entity?::	Yes
Petition Included?::	No
Secrecy Order in Parent Appl.?::	No

Applicant Information

Applicant Authority Type::	Inventor
Primary Citizenship Country::	USA
Status::	Full Capacity
Given Name::	Srinivas
Family Name::	KUMAR
City of Residence::	Cupertino
State or Province of Residence::	California

Trend Micro, Inc.
EX1002-139

Country of Residence::	USA
Street of Mailing Address::	10926 Northridge Square
City of Mailing Address::	Cupertino
State or Province of Mailing Address::	California
Country of Mailing Address::	USA
Postal or Zip Code of Mailing Address::	95014
Applicant Authority Type::	Inventor
Primary Citizenship Country::	USA
Status::	Full Capacity
Given Name::	Gurudatt
Family Name::	SHASHIKUMAR
City of Residence::	Foster City
State or Province of Residence::	California
Country of Residence::	USA
Street of Mailing Address::	618 Plymouth Lane
City of Mailing Address::	Foster City
State or Province of Mailing Address::	California
Country of Mailing Address::	USA
Postal or Zip Code of Mailing Address::	94404

Correspondence Information

Correspondence Customer Number::	21839
Phone Number::	(703) 836-6620
Fax Number:	(703) 836-2021

Representative Information

Representative Customer Number:: 21839

Domestic Priority Information

Application::	Continuity Type::	Parent Application::	Parent Filing Date::
This Application	Claiming the benefit under 35 USC 119(e)	61/443,854	02/17/11

Assignee Information

Assignee Name::	TAASERA, INC.
Street of Mailing Address::	1030 State Street
City of Mailing Address::	Erie
State or Province of Mailing Address::	Pennsylvania
Country of Mailing Address::	USA
Postal or Zip Code of Mailing Address::	16501

Signature		Date	February 17, 2012
Name	Charles F. Wieland III	Registration No.	33,096

Trend Micro, Inc.
EX1002-141

Doc Code: TRACK1.REQ
Document Description: TrackOne Request

PTO/SB/424 (12-11)

CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION UNDER 37 CFR 1.102(e) (Page 1 of 1)

First Named Inventor:	Srinivas KUMAR	Nonprovisional Application Number (if known):	
Title of Invention:	System and Method for Application Attestation		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION FOR THE ABOVE-IDENTIFIED APPLICATION.

1. The processing fee set forth in 37 CFR 1.17(i), the prioritized examination fee set forth in 37 CFR 1.17(c), and if not already paid, the publication fee set forth in 37 CFR 1.18(d) have been filed with the request. The basic filing fee, search fee, examination fee, and any required excess claims and application size fees are filed with the request or have been already been paid.

2. The application contains or is amended to contain no more than four independent claims and no more than thirty total claims, and no multiple dependent claims.

3. The applicable box is checked below:

I. ☑ Original Application (Track One) - Prioritized Examination under § 1.102(e)(1)

i. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.

---OR---

(b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper.

ii. An executed oath or declaration under 37 CFR 1.63 is filed with the application.

II. ☐ Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)

i. A request for continued examination has been filed with, or prior to, this form.
ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Signature /Charles F. Wieland III/	Date February 16, 2012
Name (Print/Typed) Charles F. Wieland III	Practitioner Registration Number 33,096

***Note**: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required in accordance with 37 CFR 1.33 and 11.18. Please see 37 CFR 1.4(d) for the form of the signature. If necessary, submit multiple forms for more than one signature, see below*.*

☑ *Total of 1 forms are submitted.

PTO/SB/96 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: Srinivas Kumar et al.

Application No./Patent No.: _____ Filed/Issue Date: February 17, 2012

Titled: SYSTEM AND METHOD FOR APPLICATION ATTESTATION

Taasera, Inc. (Name of Assignee), a Corporation (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that it is:

1. [X] the assignee of the entire right, title, and interest in;

2. [ ] an assignee of less than the entire right, title, and interest in (The extent (by percentage) of its ownership interest is _____ %); or

3. [ ] the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

the patent application/patent identified above, by virtue of either:

A. [X] An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy therefore is attached.

OR

B. [ ] A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

2. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

[ ] Additional documents in the chain of title are listed on a supplemental sheet(s).

[X] As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (*i.e.*, a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

Kumar
Signature

2/16/2012
Date

Srinivas Kumar
Printed or Typed Name

Chief Technology Officer
Title

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

ASSIGNMENT

(JOINT)

THIS ASSIGNMENT, by Srinivas Kumar and Gurudatt Shashikumar, residing at 10926 Northridge Square, Cuptertino, California 95014 and 618 Plymouth Lane, Foster City, California 94404 (hereinafter referred to as "the Assignors"), respectively, witnesseth:

WHEREAS, the Assignors have invented certain new and useful improvements in System and Method for Application Attestation set forth in an application for Letters Patent of the United States, which is a

(a) ☒ provisional application

(i) ☒ bearing Application No. 61/443,854, and filed on February 17, 2011;

(ii) ☐ to be filed herewith; or

(b) ☒ non-provisional application

(i) ☐ bearing Application No. ___, and filed on ___;

(ii) ☒ having an oath or declaration executed on even date herewith prior to filing of application;

(iii) ☐ having an oath or declaration executed on a different date than this Assignment; and

WHEREAS, Taasera, Inc., a corporation duly organized under and pursuant to the laws of Delaware, and having a principal place of business at 1030 State Street, Erie, Pennsylvania 16501 (hereinafter referred to as "the Assignee"), is desirous of acquiring the entire right, title, and interest in and to said inventions, the right to file applications on said inventions and the entire right, title and interest in and to any applications, including provisional applications for Letters Patent of the United States or other countries claiming priority to said application, and in and to any Letters Patent or Patents, United States or foreign, to be obtained therefore and thereon.

NOW, THEREFORE, for good and sufficient consideration, the receipt of which is hereby acknowledged, the Assignors have sold, assigned, transferred, and set over, and by these presents do sell, assign, transfer, and set over, unto the Assignee, its successors, legal representatives, and assigns the entire right, title, and interest in and to the above-mentioned inventions, the right to file applications on said inventions and the entire right, title and interest in and to any applications for Letters Patent of the United States or other countries claiming priority to said applications, and any and all Letters Patent or Patents of the United States of America and all foreign countries that may be granted therefore and thereon, and in and to any and all applications claiming priority to said applications, divisions, continuations, and continuations-in-part of said applications, and reissues and extensions of said Letters Patent or Patents, and all rights under the International Convention for the Protection of Industrial Property, the same to be held and enjoyed by the Assignee, for its own use and behoof and the use and behoof of its successors, legal representatives, and assigns, to the full end of the term or terms for which Letters Patent or Patents may be granted as fully and entirely as the same would have been held and enjoyed by the Assignors had this sale and assignment not been made;

AND for the same consideration, the Assignors hereby covenant and agree to and with the Assignee, its successors, legal representatives, and assigns, that, at the time of execution and delivery of these presents, the Assignors are the sole and lawful owners of the entire right, title, and interest in and to the inventions set forth in said applications and said applications, including provisional applications, above-mentioned, and that the same are unencumbered, and that the Assignors have good and full right and lawful authority to sell and convey the same in the manner herein set forth;

AND for the same consideration, the Assignors hereby covenant and agree to and with the Assignee, its successors, legal representatives, and assigns that the Assignors will, whenever

counsel of the Assignee, or the counsel of its successors, legal representatives, and assigns, shall advise that any proceeding in connection with said inventions or said applications for Letters Patent or Patents, or any proceeding in connection with Letters Patent or Patents for said inventions in any country, including interference proceedings, is lawful and desirable, or that any application claiming priority to said application, division, continuation, or continuation-in-part of any applications for Letters Patent or Patents, or any reissue or extension of any Letters Patent or Patents to be obtained thereon, is lawful and desirable, sign all papers and documents, take all lawful oaths, and do all acts necessary or required to be done for the procurement, maintenance, enforcement, and defense of Letters Patent or Patents for said inventions, without charge to the Assignee, its successors, legal representatives, and assigns, but at the cost and expense of the Assignee, its successors, legal representatives, and assigns;

AND the Assignors hereby authorize and request the attorneys of Buchanan Ingersoll & Rooney PC to insert in the spaces provided above the title of the invention, filing date, application number, and attorney's docket number of said application when known.

AND the Assignors hereby request the Commissioner of Patents to issue any and all said Letters Patent of the United States to the Assignee as the Assignee of said inventions, the Letters Patent to be issued for the sole use and behoof of the Assignee, its successors, legal representatives, and assigns.

2/16/2012	Skumar
DATE	SRINIVAS KUMAR
DATE	GURUDATT SHASHIKUMAR

ASSIGNMENT

(JOINT)

THIS ASSIGNMENT, by Srinivas Kumar and Gurudatt Shashikumar, residing at 10926 Northridge Square, Cuptertino, California 95014 and 618 Plymouth Lane, Foster City, California 94404 (hereinafter referred to as "the Assignors"), respectively, witnesseth:

WHEREAS, the Assignors have invented certain new and useful improvements in System and Method for Application Attestation set forth in an application for Letters Patent of the United States, which is a

(a) ☒ provisional application

- (i) ☒ bearing Application No. 61/443,854, and filed on February 17, 2011;
- (ii) ☐ to be filed herewith; or

(b) ☒ non-provisional application

- (i) ☐ bearing Application No. ___, and filed on ___;
- (ii) ☒ having an oath or declaration executed on even date herewith prior to filing of application;
- (iii) ☐ having an oath or declaration executed on a different date than this Assignment; and

WHEREAS, Taasera, Inc., a corporation duly organized under and pursuant to the laws of Delaware, and having a principal place of business at 1030 State Street, Erie, Pennsylvania 16501 (hereinafter referred to as "the Assignee"), is desirous of acquiring the entire right, title, and interest in and to said inventions, the right to file applications on said inventions and the entire right, title and interest in and to any applications, including provisional applications for Letters Patent of the United States or other countries claiming priority to said application, and in and to any Letters Patent or Patents, United States or foreign, to be obtained therefore and thereon.

NOW, THEREFORE, for good and sufficient consideration, the receipt of which is hereby acknowledged, the Assignors have sold, assigned, transferred, and set over, and by these presents do sell, assign, transfer, and set over, unto the Assignee, its successors, legal representatives, and assigns the entire right, title, and interest in and to the above-mentioned inventions, the right to file applications on said inventions and the entire right, title and interest in and to any applications for Letters Patent of the United States or other countries claiming priority to said applications, and any and all Letters Patent or Patents of the United States of America and all foreign countries that may be granted therefore and thereon, and in and to any and all applications claiming priority to said applications, divisions, continuations, and continuations-in-part of said applications, and reissues and extensions of said Letters Patent or Patents, and all rights under the International Convention for the Protection of Industrial Property, the same to be held and enjoyed by the Assignee, for its own use and behoof and the use and behoof of its successors, legal representatives, and assigns, to the full end of the term or terms for which Letters Patent or Patents may be granted as fully and entirely as the same would have been held and enjoyed by the Assignors had this sale and assignment not been made;

AND for the same consideration, the Assignors hereby covenant and agree to and with the Assignee, its successors, legal representatives, and assigns, that, at the time of execution and delivery of these presents, the Assignors are the sole and lawful owners of the entire right, title, and interest in and to the inventions set forth in said applications and said applications, including provisional applications, above-mentioned, and that the same are unencumbered, and that the Assignors have good and full right and lawful authority to sell and convey the same in the manner herein set forth;

AND for the same consideration, the Assignors hereby covenant and agree to and with the Assignee, its successors, legal representatives, and assigns that the Assignors will, whenever

counsel of the Assignee, or the counsel of its successors, legal representatives, and assigns, shall advise that any proceeding in connection with said inventions or said applications for Letters Patent or Patents, or any proceeding in connection with Letters Patent or Patents for said inventions in any country, including interference proceedings, is lawful and desirable, or that any application claiming priority to said application, division, continuation, or continuation-in-part of any applications for Letters Patent or Patents, or any reissue or extension of any Letters Patent or Patents to be obtained thereon, is lawful and desirable, sign all papers and documents, take all lawful oaths, and do all acts necessary or required to be done for the procurement, maintenance, enforcement, and defense of Letters Patent or Patents for said inventions, without charge to the Assignee, its successors, legal representatives, and assigns, but at the cost and expense of the Assignee, its successors, legal representatives, and assigns;

AND the Assignors hereby authorize and request the attorneys of Buchanan Ingersoll & Rooney PC to insert in the spaces provided above the title of the invention, filing date, application number, and attorney's docket number of said application when known.

AND the Assignors hereby request the Commissioner of Patents to issue any and all said Letters Patent of the United States to the Assignee as the Assignee of said inventions, the Letters Patent to be issued for the sole use and behoof of the Assignee, its successors, legal representatives, and assigns.

DATE	SRINIVAS KUMAR
2/16/2012 DATE	GURUDATT SHASHIKUMAR

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	SYSTEM AND METHOD FOR APPLICATION ATTESTATION
First Named Inventor/Applicant Name:	Srinivas KUMAR
Filer:	Charles F. Wieland III/Beverly Caraway
Attorney Docket Number:	0079152-000002

Filed as Small Entity

Track I Prioritized Examination - Nonprovisional Application under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	95	95
Utility Search Fee	2111	1	310	310
Utility Examination Fee	2311	1	125	125
Request for Prioritized Examination	2817	1	2400	2400
Pages:				
Claims:				
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Publ. Fee- early, voluntary, or normal	1504	1	300	300
Processing Fee, except for Provis. apps	1808	1	130	130
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**3360**

Electronic Acknowledgement Receipt

EFS ID:	12095148
Application Number:	13399065
International Application Number:	
Confirmation Number:	3713
Title of Invention:	SYSTEM AND METHOD FOR APPLICATION ATTESTATION
First Named Inventor/Applicant Name:	Srinivas KUMAR
Customer Number:	21839
Filer:	Charles F. Wieland III/Beverly Caraway
Filer Authorized By:	Charles F. Wieland III
Attorney Docket Number:	0079152-000002
Receipt Date:	17-FEB-2012
Filing Date:	
Time Stamp:	12:50:54
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$3360
RAM confirmation Number	10543
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

Trend Micro, Inc.
EX1002-150

1		SPEC.pdf	240029 a24d44371a77af2fb708aa23c4630553c231ece2	yes	72
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Specification		1	62	
	Claims		63	71	
	Abstract		72	72	
Warnings:					
Information:					
2	Drawings-only black and white line drawings	DRAW.pdf	978046 2eaad0d64369b7881fb355594f87971f2201f3a9	no	11
Warnings:					
Information:					
3	Oath or Declaration filed	DEC.pdf	3915833 c334b86197595ae6f9fc98c5780f1ec759f3a826	no	4
Warnings:					
Information:					
4	Power of Attorney	POA.pdf	1108445 ce8b24209e88e4ef15dbe81db1826271ea982d03	no	1
Warnings:					
Information:					
5	Transmittal of New Application	TL.pdf	83341 887f415c130f0d36468c156c821f57f11451c58d	no	2
Warnings:					
Information:					
6	Authorization for Extension of Time all replies	GENAUTH.pdf	34629 a2af58ba2664e4712afd8cb7c84ee3ff9997810c	no	1
Warnings:					
Information:					
7	Application Data Sheet	ADS.pdf	70938 dd56fe932de7e2788e80c0610d8ef2a15947126b	no	3
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					

8	TrackOne Request	424.pdf	69571 166611cafe843b22ab72b30689fc209bd1e3ccbb	no	1
Warnings:					
Information:					
9	Assignee showing of ownership per 37 CFR 3.73(b).	373b.pdf	2477936 ab5b0c659e0dc7e15d4cb0281816d8e0b999532e	no	5
Warnings:					
Information:					
10	Fee Worksheet (SB06)	fee-info.pdf	40330 f3a24424b2982ed265ac2e3d0554ca8d083e6bfc	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	9019098	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

APPLICATION FOR
UNITED STATES LETTERS PATENT

FOR

SYSTEM AND METHOD FOR APPLICATION ATTESTATION

by

SRINIVAS KUMAR
AND
GURUDATT SHASHIKUMAR

Attorney Docket No. 0079152-000002
BUCHANAN INGERSOLL & ROONEY PC
CUSTOMER NO. 21839
P.O. Box 1404
Alexandria, VA 22313-1404

SYSTEM AND METHOD FOR APPLICATION ATTESTATION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims the benefit of U.S. Provisional Appl. No. 61/443,854 entitled "SYSTEM AND METHOD FOR APPLICATION ATTESTATION," filed February 17, 2011, which is incorporated by reference herein in its entirety.

BACKGROUND OF THE DISCLOSURE

FIELD OF THE DISCLOSURE

[0002] The present disclosure relates to the field of data center virtualization and, more particularly, to a system and method to provide attestation of applications at runtime.

DESCRIPTION OF THE RELATED ART

[0003] One recent trend in computing is the trend towards cloud computing in which, for example, enterprise software is no longer owned by the customer, but instead the Information Technology infrastructure can be provided by a third party and the software applications may be sold as service offerings.

SUMMARY OF THE DISCLOSURE

[0004] The presently disclosed technology may be embodied as a method, apparatus and/or system to discover one or more applications and/or to attest for the

applications on an instrumented target platform at runtime using or based on a plurality of assertions (or statements).

[0005] The presently disclosed technology also may be embodied as a method, apparatus, and/or system for a plurality of services that enable visibility, control, and/or compliance in a cloud computing environment with dynamic application discovery, identification, monitoring and/or attestation based on a plurality of factors.

[0006] The presently disclosed technology also may be embodied as a further method, apparatus and/or system to establish user-to-application connections based on dynamic attestation of applications, and/or security controls provisioned based on context-aware business logic instead of, for example, topology based coordinates associated with encapsulation headers in network packets.

[0007] The presently disclosed technology also may be embodied as a yet further method, apparatus and/or system to authorize user-to-application transactions and/or data exchange in an established connection, during the authentication phase based on dynamic attestation of applications.

[0008] The presently disclosed technology also may be embodied as an additional method, apparatus and/or system for a runtime monitor to inspect web and non-web applications (e.g., all web and non-web applications) running on the instrumented target platform. The system may include an attestation service (or broker) using an attestation server and configured to generate application artifacts and/or to issue application statements or claims. The application artifact may represent an identified application instance (e.g., at runtime, globally, uniquely, opaquely and/or in a time-sensitive manner, for example, using an application artifact

having a specified or predetermined lifetime) on an instrumented platform (such as but not limited to a, Personal Digital Assistant (PDA), a tablet computing device, an iPhone™, an iPod™, an iPad™, a device operating the Android operating system (OS) from Google Inc., a device running the Microsoft Windows® Mobile OS, a device running the Microsoft Windows® Phone OS, a device running the Symbian OS, a device running the webOS from Hewlett Packard, Inc., a mobile phone, a BlackBerry® device, a smartphone, a hand held computer, a netbook computer, a palmtop computer, a laptop computer, an ultra-mobile PC, a portable gaming system, a gaming console, or another similar type of computing device having a computer, microprocessor). The application statements may include at least one statement (or claim) about an inspected runtime execution context and/or an intelligence based security context.

[0009] The runtime monitor may be configured to inspect the execution context of the application after using a local attestation process. The execution context of each respective application may include associated files, processes, and/or network epochs (e.g., socket events). The system may include any type of identity provider configured to authenticate a user to web or non-web applications (for example, client-server or peer-to-peer applications) based on a request for attestation of and a security context of a target application on a computing platform (e.g., the instrumented target platform).

[0010] The presently disclosed technology also may be embodied as a method, apparatus and/or system that may include a network access enforcer for controlling the authenticated user's physical access to the target application on the

instrumented target platform, responsive to one or more issued application statements (e.g., issued by the attestation service or another entity).

[0011] The presently disclosed technology also may be embodied as another method, apparatus and/or system to include an identity provider for controlling the authenticated user's authorization to commence transactions with a target application on the instrumented target platform, responsive to one or more issued application statements (e.g., issued by the attestation service).

[0012] The presently disclosed technology also may be embodied with an application artifact that may include at least a registered name (e.g., a registered globally unique security principal name) for the running application instance (e.g., a user program or a service program, among others). The attestation service may be configured to generate an artifact based on a runtime local execution context of the running application instance on the instrumented target platform.

[0013] The presently disclosed technology also may be embodied with one or more application statements or claims which may include at least one of: (1) a registered name (e.g., a registered globally unique security principal name) for the running application instance; (2) a digitally signed certificate; (3) creation and/or modification timestamps; (4) assertions of a security context from a plurality of collaboration services; (5) a list of active listening and/or open network ports (e.g., well-known and/or ephemeral); (6) network addresses used by the application; (7) a product publisher; (8) a product version; and/or (9) other runtime local execution context information.

[0014] The presently disclosed technology also may be embodied with one or more application statements or claims, which may include attribute value assertions about an introspected security context of one or more running applications. The introspected security context may be received from one (e.g., any one) of the plurality of collaboration services.

[0015] The presently disclosed technology may also be embodied with a plurality of collaboration services which may include: (1) an application whitelisting services (e.g., any application whitelisting services); (2) a vulnerability assessment service; (3) a patch management service; (4) an anti-virus service (5) a predictive and behavioral analytics engine; (6) and orchestration service; (7) a network intrusion detection or prevention service; (8) an open flow switch controller; and/or (9) a malware analysis system.

[0016] The presently disclosed technology may also be embodied with: (1) an identity provider that may include a single sign-on service or a brokered authentication service; (2) a network access enforcer, which may include devices such as for example network firewalls, load balancers, and/or VPN gateways, and which may be configured as a policy enforcement point to control access based on an application statement or claim.

[0017] The presently disclosed technology also may be embodied as a method, apparatus and/or system for evaluating authenticity of a web application (for example, a servlet in a container element). The method may include requesting a runtime application artifact for the web application from an attestation service, and requesting, based on the application artifact, an application statement from the

attestation service. The method may further include requesting from a plurality of collaboration services, for example by the attestation service, a context (e.g., an introspection based security context) for the web application on the instrumented target platform. The method may also include establishing a communication channel (e.g., a secure communications channel) between the instrumented target platform and the server providing attestation service, and generating an application statement corresponding to at least one component of the web application. The method may include generating the statement about the application components, based on a parent/child association and/or a loader dependency, and transmitting the application statement to an identity provider. The method may further include generating a multi-factor confidence metric of the web application to be included with and rendered natively by a passive web client or browser.

[0018] The presently disclosed technology may be embodied as another method, apparatus and/or system for evaluating authenticity of a non-web client-server application and/or a peer-to-peer application. The method may include requesting an application artifact for the application from an attestation service, for example, by a runtime monitor, and requesting an application statement from the attestation service, for example, by network access enforcer(s). The method may further include requesting, by the attestation service from a plurality of collaboration services, a context (e.g., an introspection based security context) for the application on the instrumented target platform. The method may also include requesting a notification of or subscribing to a change (e.g., any change) in the execution context of the application on the instrumented target platform. The method may additionally

include generating and publishing one or more application statements or claims about (regarding) the application based on at least one of a subscription request by a plurality of identity providers and/or network access enforcers. The method may further include receiving or generating, and publishing a multi-factor confidence metric of the application for a physical or logical access control decision.

[0019] The presently disclosed technology also may be embodied as a method, apparatus and/or system for client-server and/or peer-to-peer applications to evaluate the authenticity of peers prior to commencing a transaction or data exchange (e.g., any transaction or data exchange). The method may include a client-server application and/or a peer-to-peer application that may request an application artifact for each of the applications from an attestation service (or attestation server), and further may request, based on an artifact exchange, one or more application statements from the attestation service for each peer application. The method may further include requesting, by the attestation service from a plurality of collaboration services, a context (e.g., an introspection based security context) for these applications on the instrumented target platforms. The method may further include a secure exchange of the issued application artifacts between the applications, and a verification process (such as a back-channel verification of the exchanged artifacts with the attestation service). This method may further include requesting one or more application statements, based on (or responsive to) the exchanged application artifact, from the attestation service, and determining by the peer applications, or by the network access enforcer(s) receiving the one or more

application statements, responsive to receiving the application statements, the authenticity of the other, or each application in the transaction.

[0020] The presently disclosed technology also may be embodied as a method, apparatus and/or system for displaying and continuously updating in real time or near real time (e.g., within a threshold period) the identity, attribution, and/or attestation information of executing or running (e.g., all running) applications hosted in the private an/or public virtual data centers in a cloud computing infrastructure. The method may include displaying one or more classification based confidence metrics and active listening and/or open network ports (e.g., well known and ephemeral) assigned on a plurality of instrumented target platforms.

[0021] The presently disclosed technology also may be embodied as a method, apparatus and/or system for establishing access control policies based on a user authentication method, a user role, a dynamically discovered and attested application running on an instrumented target platform via subscription based application statements from an attestation service. The method may also include decoupling of the business logic (role based access controls, authentication requirements, and/or line of business applications, among others) from the network topology based physical constraints in the network fabric (e.g. IP addresses, MAC addresses, VLAN identifiers, and/or subnet addresses, among others) and may include context-aware logical attributes (user identity and/or application identity among others) in policy grammar. The method may further include establishing access control rules that may leverage classification based dynamic confidence

metrics, which may be included in an application statement used for authorization decisions.

BRIEF DESCRIPTION OF THE DRAWING FIGURES

[0022] The invention is best understood from the following detailed description when read in connection with the accompanying drawings. According to common practice, various features/elements of the drawings may not be drawn to scale. Common numerical references represent like features/elements. The following figures are included in the drawings:

FIG. 1 is a schematic diagram illustrating an exemplary system/architecture in accordance with various exemplary embodiments;

FIG. 2 is a schematic diagram illustrating a method of monitoring and attesting applications in a cloud computing environment in accordance with various exemplary embodiments;

FIG. 3 is a schematic diagram illustrating another method of monitoring and attesting applications in the cloud computing environment in accordance with various exemplary embodiments;

FIG. 4 is a schematic diagram illustrating a further method of monitoring and attesting applications in a cloud computing environment in accordance with various exemplary embodiments;

FIG. 5 is a schematic diagram illustrating a method of monitoring and attesting a Simple Authentication and Security Layer (SASL) enabled client and server application in accordance with various exemplary embodiments;

FIG. 6 is a schematic diagram illustrating an exemplary security administration console including an integrity dashboard in accordance with various exemplary embodiments;

FIG. 7 is a schematic diagram illustrating another exemplary policy administration console including an authorization dashboard in accordance with various exemplary embodiments;

FIG. 8 is a flowchart illustrating a method in accordance with various exemplary embodiments of the presently disclosed technology;

FIG. 9 is a flowchart illustrating a method in accordance with various exemplary embodiments of the presently disclosed technology;

FIG. 10 is a flowchart illustrating a method in accordance with various exemplary embodiments of the presently disclosed technology;

FIG. 11 is a flowchart illustrating a method in accordance with various exemplary embodiments of the presently disclosed technology;

FIG. 12 is a flowchart illustrating a method in accordance with various exemplary embodiments of the presently disclosed technology; and

FIG. 13 is a flowchart illustrating a method in accordance with various exemplary embodiments of the presently disclosed technology.

FIG. 14 is a diagram of an example computer system in which embodiments can be implemented.

DETAILED DESCRIPTION

[0023] Although the invention is illustrated and described herein with reference to specific embodiments, the invention is not intended to be limited to the details shown. Rather, various modifications may be made in the details within the scope and range of equivalents of the claims and without departing from the invention.

[0024] Many enterprises are moving there IT infrastructures to cloud computing environments (e.g., in which third parties may provide shared computing resources and applications running on those resources are offered as services to a plurality of customers) for various reasons including: (1) increased computing power; (2) increased storage capacity, and/or (3) increased network bandwidth, among others. Enterprise applications and mission critical applications may be executed in the cloud. Without adequate system and application security, the cloud can compromise these applications causing large financial losses. Data confidentiality, data integrity and data availability can be maintained in the cloud computing environment even when such applications may be controlled by these third parties. For example, enterprises are moving from self-managed on-premise data centers to service–provider managed outsourced virtual data centers (e.g., the cloud computing environments). The cloud may enable traditional information technology systems and applications to transparently execute from these service–providers managed outsourced virtual data centers. As newer technologies emerge, the cloud infrastructure may evolve transparent to and scalable with enterprise operations. Security in such environments may be an emerging challenge.

[0025] In certain exemplary embodiments, applicants may be secured by signing-on or authenticating applications onto the network using an attestation process (e.g., via a single factor or multi-factor attestation). In a multi-factor process, applications may be qualified based on at least two factors. A first factor may identify one or more attributes of the application (e.g., run time instance of the application) such as (1) a hash of the application, as an application fingerprint, (2) other applications/processes called by the application, (3) ports used by the application, (4) computing, storage, and network resource usage by the application, and/or (5) the platform executing the application, among other. Such information may be available locally (e.g., at the computing platform running the application) in the current execution context. A second factor may identify what is known about the application based on the attributes of the application from security intelligence external to the operating environment (e.g., a third party (e.g., trusted third party) separate from the computing platform running the application).

[0026] Applications that are hosted in self-managed and in-house enterprise data centers may be gradually migrating to outsourced service provider managed virtual data centers in private/public clouds. There may be a loss of visibility and direct control from this migration. Various exemplary embodiments include instrumentation to monitor the applications in process to increase visibility and enable attestation of applications executing in the outsourced service provider managed virtual data centers. As web and multi-tier applications proliferate in the cloud, secure connectivity, based on certificates issued by third party certificate authorities may be

inadequate for security and compliance because a significant number of web-based threats originate from trusted web sites.

[0027] Generally, access control mechanisms are based on static context and physical constraints rather than logical attributes and dynamic local execution context and/or a holistic security context (e.g., based on both local execution context as well as security intelligence). Physical and logical access controls based on user-to-application bindings, as an operative element of business logic, and logical attributes in a virtualized and fluid network may be used in a cloud computing environment (for the utility based infrastructure, platform and/or software as a service model) to scale and/or be viable for multi-tenancy or shared resources with deterministic confidentiality between or among tenants.

[0028] The access control mechanism may include an instrumented target (hosting) computing platform, a policy statement (e.g., grammar) based on a runtime base of the particular application, a temporal and environmental context independent of physical constraints or enforcement methods, an attestation broker (service or server) for notifying interactive users, network access enforcers and identity providers.

[0029] The confluence of single-sign-on (SSO) mechanisms and multi-tier applications (for example, the web, application, database tiers) may introduce higher risks of non-compliance in outsourced multi-tenant cloud services infrastructures. In the absence of reliable application attestation methods, impersonation and delegation of user's credentials may pose serious security threats in, for example,

multi-hop transitive chain of services, for both intra-cloud and inter-cloud computing environments, where inter-service transactions may be based on implied trust.

[0030] FIG. 1 is a schematic diagram illustrating an exemplary network 150 in accordance with various exemplary embodiments.

[0031] Referring to FIG. 1, the exemplary network 150 may include a runtime monitor 102 that may discover and identify a web-based application 103 or non-web-based application 104 that may be executing or running on a computing platform (or an instrumented target platform) 100, an attestation broker 109 that may receive a request to attest to the identify of a running application and that may query one or more collaboration services 110 to request a context (e.g., a security context and/or an introspection based security context) of the running application. The application may be an application targeted for use by an access requestor 114 (e.g., another computing platform) that may be operated by a user (or end-user) 115 via, for example an active or passive client application 116, that may desire an assurance or an attestation that the application is appropriate to be used.

[0032] The attestation broker 109 (or the collaboration service 110) may be configured to generate application statements or reports 117, which may include assertions about the running target application, and may deliver the statements or reports 117 to the requestor, the third party, and/or end-user. The platform 100 may include any computing device 101 and/or virtual platform, for example, (e.g., a computer, microprocessor, Personal Digital Assistant (PDA), smartphone, notebook computer, and/or a virtual server running on hardware, among others). The computing device may include a microprocessor 130 for execution, for example, of

computing platform software such as operating system software, applications, and runtime monitor software, among others and a memory 140 for data, metadata, and software storage.

[0033] The attestation broker 109 may issue application artifacts 107 (e.g., that may maintain a record of the state of the discovered or identified applications running on the instrumented platform 100) to the runtime monitor 102 for discovered or identified applications running on the instrumented platform 100. The runtime monitor 102 may use the application artifacts 107 to generate attribute value assertions (e.g., assertions regarding one or more attribute values associated with each respective running application) to describe the application execution context 105 of the applications.

[0034] For example, the attestation service or apparatus may include a processing unit 135 for: (1) receiving remote from the computing platform 101, a runtime execution context 105 indicating attributes of the application at runtime, and a security context 111 providing security information about the application; (2) generating a report 117 indicating security risks associated with the application based on the received runtime execution context 105 and the received security context 111, as an attestation result; and/or (3) sending the attestation result associated with the application; and a memory 145 for storing the generated report.

[0035] As a second example, the runtime monitor or monitoring apparatus may include: a processing unit 130 (e.g., a processor shared with the computing platform 101 or a separate processor) for: (1) generating a runtime execution context 105 indicating attributes of the application at runtime; (2) sending the runtime execution

context 105 to the attestation service or server 109; (3) receiving an application artifact 107 for tracking subsequent changes to the runtime execution context 105; and/or (5) updating and sending using the application artifact 107, the runtime execution context 105, as an updated execution context, responsive to the attributes of the application indicating a change; and a memory 140 for storing the application artifact 107.

[0036] The application artifact may include previous assertions or may provide an identifier that associates the application to the previous assertions. The application execution context 105 may include at least a base (or static), temporal (or dynamic) and/or environmental aspects or attributes of the target application. A requestor (for example, a network access enforcer 113, such as a network firewall, a load balancer, a VPN gateway, and/or an identity provider 112, such as an Security Token Service (STS), Single Sign On (SSO) solution may subscribe for application statements or reports 117 from the attestation broker 109.

[0037] In certain exemplary embodiments, the generation of attribute value assertions for the application execution context 105 by the runtime monitor 102 on the instrumented platform 100 may include, for example, the collection of file hash digests and/or file attributes (e.g., file size, publisher details, creation and/or modification timestamps, digital signings, and product versions) for loaded (e.g., all loaded and/or in process) components of the running target application 103 or 104. The application execution context 105 may include parent-child process associations and/or loader dependencies, information about active listening and/or open network ports that are well known or ephemeral. The application execution context 105 may

also include the executable file binaries. The runtime monitor 102 may generate and report the collection in a digitally-signed report to the attestation broker 109 in an application execution context notification.

[0038] In certain exemplary embodiments, as an outcome of (or based on) the evaluation of the running target application 103 or 104 on the target instrumented platform 100 using collaboration services 110, the attestation broker 109 may issue application statements or reports 117 via application statement notification 118. The issued application statements or reports 117 may be digitally-signed, and may include a name of the application instance (e.g., a globally unique security principal name of the application instance or other application identifier), as its application identifier. The application instance may be a user program or a service program. One example of such a name may be "service/hostname@realm".

[0039] The application statements or reports 117 may include attribute value assertions that may describe the runtime execution context 105 and application security context 111 of the application instance on the instrumented platform 100, as a machine identifier. The application identifier may be a publisher designated product name or a registered service principle name in a services directory. The machine identifier may be an IPv4/IPv6 address, a directory network services (DNS) hostname, a MAC address, a serial number (e.g., an IT or manufacturer issued serial number), an RFID, and/or other device identifiers, among others. The attestation broker 109 may provide to the requestor 112, 113 or 114, a confidence metric that may include one or more ratings (e.g., application confidence ratings for the targeted application).

[0040] The confidence metric may, for example, be classified based on: (1) the vulnerability of the application, (2) compliance of the application, (3) referential integrity of the application, and/or (4) patch level of the target application. These ratings may be determined by the attestation broker 109 based on communications or interactions with one or more of the plurality of collaboration services 110. The confidence metrics may include a value for each classification and/or an overall value, which is weighed by classification or averaged. The weighing may be predetermined, preset or determined based on user input. The confidence metrics may be a numerical representation of the evaluation of one or more of the collaborative services 110.

[0041] In certain exemplary embodiments, the application statements or reports 117 may be used by passive clients 116 (for example, a web browser) to render an icon or other indicator (either visual on the web page or audio indicator, for example, an icon at the bottom of the web page). The indicator may be an indicator (or an attestation) of the web application's authenticity to the user 115. For example, the user 115 may click on the attestation icon to view web application specific information issued by the attestation broker 109 for the accessed web application. The attestation broker 109 may be a third party independent and trusted entity that provides such attestation services. The user 115 may confirm that the application attestation offered by the attestation broker 109 is current (e.g., that the lifetime of the application attestation has not expired).

[0042] The user 115 or access requestor 114 (e.g., the computing platform of the user) may ascertain from the attestation broker 109 that the application statements

or reports (or claims) 117 represent a recently (e.g., a most recent) verified contextual assessment of the accessed web application based on timestamps and/or message sequencing in the application statements 117. The determination that the claims represent the most recent verified contextual assessment may be based on consolidating information collected via one or more of a plurality of collaboration services 110.

[0043] The application statements or reports 117 may be received and may be interpreted by one or more network access enforcers 113 (e.g., network firewalls, load balancers, and/or VPN gateways, among others), one or more identity providers 112 (e.g., STS, and/or SSO services, among others) and/or active clients 116 (e.g., Simple Authentication and Security Layer (SASL) enabled client-server and/or peer-to-peer applications, among others) to leverage contextual information about the target application 103 or 104 on the instrumented platform 100.

[0044] The runtime monitor 102 may discover, may identify and may track process starts (e.g., all process starts), process terminations (e.g., all process terminations) and network epochs (e.g., socket events) of applications on the operating system 120 of the instrumented platform 100. The local execution context of the running application may be determined at runtime and may be reported as attribute value assertions over a communication channel 106 to the attestation broker service 109.

[0045] In certain exemplary embodiment, the communication channel 106 may be a secure communication channel and/or the communication may be secured via known encryption/decryption methods. The attestation broker 109 may request

introspection based security context (for example, evaluations and behavioral or predictive analytics based on historic state information and measurements sampled over a period of time using a variety of inspection methods) for the running application on the instrumented platform 100 from one or more of the plurality of collaboration services 110.

[0046] In certain exemplary embodiments, the collaboration services 110 may perform just-in-time inspection (e.g., an assessment scan) of the target application and platform 100. The collaboration service 110 may lookup the most recent inspection report based on, for example, an IT service management schedule and may return the requested attestations pertaining to the application execution context 105 to the requestor 112, 113 or 114 or the user 115.

[0047] The attestation broker 109 may generate and may return an application artifact 107 for the running application 103 or 104 to the runtime monitor 102, as a reference for subsequent execution context change notifications 207 (see FIG. 2) for the applications. Changes (e.g., any changes) in the running application's local execution context 105 may trigger an interaction with the attestation broker 109 (e.g., a communication by the runtime monitor 102 to the attestation broker 109) to reissue the application statements or reports 117 for attestation of the targeted application having the changed local execution context. For example, when the hash of the targeted application changes or the file size of the targeted application changes, an updated attestation may be initiated by the runtime monitor 102 and provided by the attestation broker 109. The attestation broker 109 may query one or more of the

collaborative services 110 to determine the updated application statement or report 118 associated with the changed targeted application.

[0048] In certain exemplary embodiments, the attestation broker 109 may provide a single confidence value that represents the confidence (or risk) regarding the authenticity of the targeted application or a confidence metrics of a plurality of values based on different (e.g., independent) classifications. In other exemplary embodiments, the attestation broker 109 may provide the confidence metrics and other information in a standard format such that the requestors 112, 113 and/or 114 or the runtime monitor 102 may analyze various attributes of the other information. For example, the runtime monitor 102 may store or may have access to application attestation policies and may compare the local execution context and application statement or report 117 with the attestation policies to determine whether the targeted application is authenticated for use by the requestor. The identity provider 112 may receive, for example, a web redirect from web application 103 to perform brokered authentication ceremonies to login a user (e.g., an interactive user) 115.

[0049] In certain exemplary embodiments, the web application 103 may request via an application artifact request 106 an application artifact 107 from the attestation broker 109. The web application 103 may include the received application artifact 107 in a web redirect to the identity provider 112. The identity provider 112 may perform a back-channel query 118 to validate that the received application artifact 107 had been issued by the attestation broker 109 to ascertain the authenticity of the web application 103. The identity provider 112 may then receive application statements or reports 117 for the web application 103. A visual, audio or

programmatic indication of application attestation may be provided to the access requestor 114 or user 115 via the access requestor 114.

[0050] The interactive user 115 or requestor 114 may receive a visual or audio attestation of application authenticity, for example, in the form of a visual indicator or an icon on the login form. The attestation may be accepted or rejected before proceeding with any transaction with the web application 103 or the attestation may be automatically accepted after a predetermined or user specified time period, if not rejected by the user 115 or requestor 114.

[0051] A network access enforcer 113 may subscribe with the attestation broker 109 for application statements or reports 117 and may discover a plurality of target applications 103 or 104 on a plurality of target machines or platforms 100. The communication protocol for the communications 118 between the attestation broker 109 and the network access enforcer 113 may be any standards based protocol and message exchange data structures or schemas, such as for example: (1) Simple Object Access Protocol (SOAP); (2) Representational State Transfer (REST); or (3) Trusted Computing Group's (TCG's) Interface for Metadata Access Points (IF-MAP) specification, among others.

[0052] The attestation broker 109 may publish notifications with real time or near real-time application statements or reports 117 for the network access enforcer 113 to apply physical access controls (e.g., controls to physically enable access to or to block access to the targeted application). The determination to enable or disable physical access by the network access enforcer 113 may be based on attribute value assertions (e.g., in the transport layer) in application statements or records 117. The

attribute value assertions may include for example, static (e.g., well known) and/or dynamic (e.g., ephemeral) network ports assigned to the target application 103 or 104.

[0053] An active client application 116 and/or a server application 104 (e.g., using the Simple Authentication and Security layer (SASL) protocol) may request and/or use the received application statements or reports 117 programmatically for a mutual attestation handshake. For example, using SASL protocol such a mutual attestation handshake may be defined by an integrity exchange profile, before initiating an authentication handshake with proof of possession of credentials.

[0054] FIG. 2 is a schematic diagram illustrating a method of monitoring and attesting applications in a cloud computing environment in accordance with various exemplary embodiments.

[0055] Referring to FIG. 2, an exemplary network 250 may include a runtime monitor 201, an instrumented target platform 200, an attestation broker 202, a metadata database 210, and/or a plurality of collaboration services 203.

[0056] The runtime monitor 201 may discover, may inspect, may identify and/or may attest to the runtime execution of applications on the instrumented target platform 200. The attestation broker 202 may issue application artifacts 206 based on a received application execution context (or application execution context change notification) 207 for registered application instances 204. Responsive to the request from the runtime monitor 201, or an access requestor 114 or user 115, the attestation broker (or attestation server) 202 may initiate a query 205 of one or more of the plurality of collaboration services (or collaboration servers) 203. The query

205 may include a search for a security context (e.g., an introspection based security context) for the target application.

[0057] In certain exemplary embodiments, the applications running on the instrumented target platform 200 may be verified using one or more of the collaboration services 203 for identification, based on an application execution context received from the runtime monitor 201 either directly or via the attestation broker 202.

[0058] The runtime monitor 201 may inspect the execution context of processes on the instrumented target platform 200 for application epochs (e.g., process and/or socket events). Responsive to or after detection of application process start, a runtime application execution context (e.g., metadata) may be generated. The metadata may include: (1) the file hash digest, (2) file attributes (for example, the file size, the publisher details, the creation and/or the modification timestamps, the digital signing, and/or the product version) for loaded components of the running target application, (3) parent-child process associations, (4) loader dependencies, and/or (5) information about active listening and/or open network ports that may be well-known and/or ephemeral; and/or executable file binaries. The running application may be registered 204 by providing the generated application execution context to the attestation broker 202.

[0059] In certain exemplary embodiments, the attestation broker 202 may verify the authenticity of the running application on the instrumented target platform 200 with the query 205. The query 205 that may include the metadata collected from the runtime monitor 201 may be sent from the attestation broker 202 and received by

one or more collaboration services 203. The query 205 may request a security context for the running application that may indicate the level of risk (of confidence) associated with running the target application on the instrumented platform 200.

[0060] The attestation broker 202 may generate a dynamically changing application artifact 206 which may be time sensitive and may be globally unique. The application artifact 206 may be based on the received application execution context and the attestation broker 202 may return the generated application artifact to the runtime monitor 201. The runtime monitor 201 may inspect each of the running applications for state changes including, for example, active listening and open network ports (e.g., well-known and ephemeral) and/or terminations of the applications. These inspections may occur, for example, at the transport layer of the open systems interconnection (OSI) stack.

[0061] In certain exemplary embodiments, other types of state changes may be inspected, such as elements related to the execution context. Any contextual (state) changes may be notified in real time or near real time by an application execution context change notification 207 from the runtime monitor 201 to the attestation broker 202. The attestation broker 202 may store persistent and/or transient state information (e.g., including metadata) in a local database or remote repository 210, such as an IF-MAP Server, for example) for registered applications (e.g., each registered running application) on one or more of the plurality of instrumented target platforms 200.

[0062] FIG. 3 is a schematic diagram illustrating another method of monitoring and attesting applications in the cloud computing environment in accordance with various exemplary embodiments.

[0063] Referring to FIG. 3, an exemplary network 350 may include an interactive user 300, an instrumented target platform 301, a web application 302, an identity provider 303, an attestation broker 304 and collaboration services 305. The web application 302 may interact with the attestation broker 304 for runtime multi-factor attestation of the web application 302. The operational flow may enable a mechanism to apply, for example, at a post-connect phase of a session for authorization control on an intermediate node element in the control path.

[0064] The interactive user 300 may establish a physical connection over a network and may initiate an application access request 306 to commence or initiate a transaction with a web application 302 hosted on the instrumented target platform 301.

[0065] In certain exemplary embodiments, the web application 302 may execute a code element (such as for example, a web servlet or other processing element) that may generate a runtime application execution context (e.g., metadata) and may automatically initiate a query 307 to the attestation broker 304 by sending the generated metadata of the runtime application execution context.

[0066] In certain exemplary embodiments, the attestation broker 304, may verify the authenticity of the running web application 302 on the instrumented target platform 301 by sending a verification query 311 (e.g., real time or near-real time) of the received metadata to one or more of the collaboration services 305 and receiving

from the queried collaboration services 305 an application security context 312. The attestation broker 304 may generate an application artifact 308 and may send the application artifact to the web application 302.

[0067] The web application 302 may include (for example, may embed, as a markup) the received application artifact 309 as an assertion (e.g., in a security assertion markup language (SAML or other common form of markup)) to the identity provider 303 which may use back-channel communications 310 with the attestation broker 304 to verify the application artifact 309.

[0068] In certain exemplary embodiments, the attestation broker (or attestation server) 304 may request a collaboration service 305 for an introspection based security context for the running application.

[0069] In various exemplary embodiments, the identity provider 303 may initiate a direct interactive authentication sequence with an interactive user 300 in the associated domain (e.g., realm). The login form (or web page) displayed to the user 300 may include an application attestation 313. The application attestation 313 may be in any perceivable indicator including an attestation icon for the accessed web application. For example, the attestation icon may include information about the web application 302, such as, for example, the identity, the product version, the publisher, the modification timestamp, and/or the confidence metrics. The user 300 may determine whether the information including the confidence metrics information is acceptable to continue with the transaction (e.g., to use of the running target application) and may provide proof of possession of credentials 314 to authenticate the user 300 to the identity provider 303.

[0070] Although user authentication is disclosed as occurring after the determination whether to continue the transaction to use the running application, it is contemplated that user authentication may occur at any stage of the login process and may occur prior to such a determination whether to use the running application.

[0071] In certain exemplary embodiments, values associated with the confidence metrics may be provided on a common scale (e.g., a scale of 1 to 10) and may be presented to the user 300 with a common visual scheme such as green to indicate a low risk for use of the target application, yellow to indicate a intermediate risk for use of the target application, and red to indicate a high risk for use of the target application.

[0072] In certain exemplary embodiments, the identity provider 303 may query 315 the attestation broker 304 to determine whether access to the web application 302, based on an authorization profile configured for the attestation broker 304, can be granted for the authenticated user 300 to transact data exchanges with the web application 302.

[0073] In various exemplary embodiments, the identity provider 303 may return standards based authentication, attribute and/or authorization statements or reports 316 to the web application 302. The web application 302 may selectively grant access to the user 300 for the target application on the instrumented platform 301 or may selectively block access by the user 300 to the target application on the instrumented platform 301 based on the application statements or reports 316 received from the attestation broker 304 and pre-established or system administrator established access or attestation policies.

[0074] The application statements or reports 316 may include, for example, information about the user's identity, one or more authentication factors such as password, PIN, smart card, among others, and preexisting roles in a user directory (for example, Active Directory, among others), a role based management system (for example, Oracle or SAP, among others) and/or a relational database (for example, MS-SQL, MySQL, or Oracle DB, among others). Access may also be granted or denied (blocked) based on a plurality of factors.

[0075] For example, the identity provider 303 may deny access to an authenticated user 300 based on the level of concern (e.g., high) in the confidence metrics for a specific classification (e.g., compliance). The level of concern for a classification of the confidence metrics may be expressed in user-to-application policy bindings provisioned for the attestation broker 304. The outcome of the policy decision logic, at or external to the attestation broker 304, may be returned to the web application 302, as one or more application statements or reports.

[0076] The identity provider 303 may represent an intermediate single sign-on (SSO) entity (or function) that may use identity stores (or caches) to manage passwords and may perform authentication ceremonies on behalf of the user 300. The authentication may be performed such that it is transparent to the user 300.

[0077] FIG. 4 is a schematic diagram illustrating a further method of monitoring and attesting applications in a cloud computing environment in accordance with various exemplary embodiments.

[0078] Referring to FIG. 4, an exemplary network 450 may include an instrumented target platform 400, a runtime monitor 401, an attestation broker 402,

collaboration services 403, an interactive user 404, and/or a network access enforcer 405. The user 404 may establish a physical connection over network 450 and may initiate an application access request 411 to commence or initiate a transaction with a target application hosted on the instrumented target platform 401.

[0079] Applications running on the instrumented target platform 400 may be inspected by the runtime monitor 401 for application execution context and state changes. The operational flow may be an exemplary mechanism to apply, during or at the connection establishment phase of a session (e.g., an Internet Protocol (IP) or non-IP session), authorization controls at an intermediate system or apparatus in the data path.

[0080] The runtime monitor 401 may inspect the instrumented target platform 400 for application epochs (e.g., process and/or socket events). Responsive to detection of an application process start by the run-time monitor 401, the runtime monitor may generate a runtime application execution context (e.g., metadata), which may include, for example, the file hash digests and/or file attributes for loaded components of the running target application. The running target application may be registered by the runtime monitor 401 with the attestation broker 402 via a start notification 406 and the runtime application execution context (e.g., that may include the metadata) may be sent by the runtime monitor 401 to the attestation broker 402 via an application execution context change notification 408. In certain exemplary embodiments, the notifications 406 and 408 may occur together.

[0081] In certain exemplary embodiments, the attestation broker 402 may verify the authenticity of the running application on the instrumented target platform 400

with a real time or near real time exchange 409 of the received metadata with one or more collaboration services 403 and the return of the application security context 410 based on the exchanged metadata. The attestation broker 402 may also request on or more collaboration services 403 to perform a static, dynamic and/or virtual execution analysis of the executable file binary, for example, by a malware analysis system.

[0082] In certain exemplary embodiments, the attestation broker 402 may remediate an instrumented target platform 400, using manual or automated methods, in response to a requested analysis performed by one or more collaboration services 403.

[0083] The attestation broker 402 may generate a dynamic application artifact (e.g., that may be globally unique and may be time-sensitive) 407 and may issue the application artifact 407 to the runtime monitor 401. The runtime monitor 401 may inspect running applications on the instrumented target platform 400 for contextual (state) changes, including, for example, active listening and/or open network ports, (e.g., at the transport layer of the OSI stack), and terminations of applications.

[0084] In certain exemplary embodiments, other types of state changes may be inspected, such as elements related to the execution context. Contextual (or state) changes 408 (e.g., any contextual changes) may be notified in real time or near real time to the attestation broker 402. The attestation broker 402 may store persistent and transient state information in a local database or remote repository 210 (see FIG. 2) for registered running applications on a plurality of instrumented target platforms 400.

[0085] A network access enforcer 405 may register or subscribe with the attestation broker 402 as a web service over a web services protocol interface 412:413 for notifications (e.g., publications) of application statements or reports (e.g., claims) for running applications (e.g., all running applications) on a plurality of instrumented target platforms 400. The attestation broker 402 may publish in real time or near real time, up-to-date application statements or reports 413 to a plurality of subscribers 405 or users 404. The application statements or reports may include (1) an application identifier such as a registered name (e.g., a globally unique service principle name), (2) a machine identifier, (3) a product identifier, (4) a product version, (5) active listening and/or open network ports, (6) network addresses used by the target application, and/or (7) confidence metrics based on security context assessments 410 performed by one or more collaboration services 403. The confidence metrics may be based on: (1) recent (e.g., the most recent) security context assessments performed by one of the collaboration services 403, (2) correlated data from different collaboration services 403, and/or (3) weighed averages associated with each security context assessment, among others.

[0086] The network access enforcer 405 may query the attestation broker 402 for user specific application bindings configured for the attestation broker 402 to determine authorization controls based on dynamic multi-factor application attestation, and real time (or near real time) confidence metrics based on the local execution context 408 and assessed security context 410. For example, the network access enforcer 405, such as a virtual or physical network firewall appliance, may deny access to an authenticated user based on the level of concern ("high") (for

example, from a three level ranking system of "high", "medium" and "low") in the confidence metrics for a specific classification (e.g., patch level) as expressed in the user-to-application policy bindings provisioned for the attestation broker 402. Although a three level ranking system is illustrated, it is contemplated that ranking systems with more or less levels are possible.

[0087] FIG. 5 is a schematic diagram illustrating a method of monitoring and attesting a Simple Authentication and Security Layer (SASL) enabled client and server application in accordance with various exemplary embodiments.

[0088] Referring to FIG. 5, an exemplary network 550 may include a client application 500, a server application 501, an attestation broker 502, a collaboration service 503, and/or an application programming interface (API) library 516.

[0089] Although a Simple Authentication Security Layer (SASL) protocol is illustrated, it is contemplated that any application layer protocol between client-server and peer-to-peer applications, or network security protocols, for example IPSec Authenticated Internet Protocol (AuthIP) or Internet Key Exchange (IKE), may be extended and/or used to provide the functions of the client application 500 and the server application 501.

[0090] In certain exemplary embodiments, the client application 501 and the server application 501 may be statically or dynamically linked to the API library 516 (e.g., a Trust-as-a-Service (TAAS) API library). The API library 516 may implement a set of procedure calls for applications to exchange messages (e.g., opaque and/or secure messages) with an attestation service or broker 502 that may hide the implementation details from the higher level application.

[0091] Although one exemplary embodiment is illustrated for the API library 516, it is contemplated that any application framework may be extended to implement the set of procedure calls provided by the API library 516.

[0092] The server application 501 may send a runtime server application execution context 504, may request a server application artifact 505, and may receive the server application artifact 505 from the attestation service (e.g., the attestation broker or the attestation server) 502. The application execution context 504 may include the file hash digests and file attributes of components of the running server application 501 including parent-child process associations and loader dependencies.

[0093] The client application 500 may establish a network connection to the server application 501 and may initiate a profile exchange for authentication.

[0094] Subsequent to completing an authentication exchange (for example to authenticate the user associated with the client application 500), the client application 500 may send a runtime client application execution context 506 and may request a client application artifact 507 from the attestation broker or service or server 502. The client application execution context 506 may include the file hash digests and file attributes of components of the running client application 500 including parent-child process associations and loader dependencies. Responsive to or after receiving a client application artifact 507, the client application 500 may transmit the received application artifact (indicated as 508) to the server application

501. The server application 501 may send the received client application artifact 507 to the attestation server 502 for client artifact validation 509 and may request a client application statement or report 511 for the client application 500.

[0095] In certain exemplary embodiments, the attestation broker 502 may initiate a request 520 for an introspection based security context 510 for the client application 500 from one or more of the collaboration services 503. The requested collaboration services 503 may collect and may generate the client application security context 510 and may send the client application security context 510 to the attestation broker 502. The client application statement or report 511 may be generated by the attestation broker 502 from the client application security context 510 and may include assertions about the runtime execution context 504 and intelligence based security context 510 for the client application 500. Responsive to receiving the client application statement or report 511 from the attestation server 502, the server application 501 may determine whether the attestation of the client application 500 is adequate.

[0096] In certain exemplary embodiments, the confidence metrics may be included in the client application statements or reports 511 and may be analyzed, for example by the server application 501, to determine whether to transact data exchanges with the client application 500.

[0097] Upon or after receiving the client application statements 511 and determining to transact data exchanges with the client application 500, the server application 501 may transmit the received server application artifact (indicated as 512) to the client application 500. The client application 500 may send the received server application artifact 512 to the attestation server 502 for validation of the server artifact 513 and may request an application statement or report 515 for the server application 501.

[0098] In certain exemplary embodiments, the attestation broker 502 may initiate a request 519 for an introspection based security context 514 for the server application 501 from one or more of the collaboration services 503. The requested collaboration services 503 may collect and may generate the server application security context 514 and may send the server application security context 514 to the attestation broker 502. The server application statement or report 515 generated by the attestation broker 502 may include assertions about the runtime execution context and intelligence based security context for the server application 501. Responsive to or after receiving the server application statement or report 515 from the attestation broker or service 502, the client application 500 may determine whether the attestation of the server application 501 is adequate. In certain exemplary embodiments, the confidence metrics included in the server application

statement may be analyzed, for example by the client application, to determine whether to transact data exchanges with the server application 501.

[0099] Although confidence metrics included in the application statements may be analyzed by the requesting application, in certain exemplary embodiments, the API library 516 may provide standard and/or custom pluggable filters to normalize the classifications based confidence metrics such that a standard rating scale may be provided to each requesting application and the requesting application may predetermine settings for denying access to an application with a particular rating exceeding a risk threshold and/or granting access to the application with the particular rating equal to or not-exceeding the risk threshold. In certain exemplary embodiments, application at or near the risk threshold may be temporarily denied access pending further analysis based on additional collaborative services 503 or based on user of system administrator input granting or denying such access.

[0100] FIG. 6 is a schematic diagram illustrating an exemplary security administration console 650 including an integrity dashboard 600 in accordance with various exemplary embodiments of the invention.

[0101] Referring to FIG. 6, the exemplary security administration console 650 may visually display the integrity dashboard or display window 600. The integrity dashboard or display window 600 may include information fields including a

dashboard clock 601, discovered and identified applications 602, service realms 603, instrumented target platforms 604, product vendors 605, product versions 606, active network service ports 607, and confidence metrics 608.

[0102] The information fields may be displayed and/or updated in real time or near real time. For example, the identified and attested application 602 running on the instrumented target platform 604, service realms 603, product vendors 605, product versions 606, current classifications based confidence metrics 608 and currently active network service ports 607 for the application may be displayed on an integrity dashboard 600 in near real time as indicated by the dashboard clock 601. The dashboard 600 may include administrative controls (not shown) to create filters for perspective views, and issue security alerts based on a plurality of defined criteria and/or provide companion reporting services.

[0103] Although the integrity dashboard is shown with specific information fields and in a particular arrangement, it is contemplated that other information fields and arrangements are possible. For example, additional attributes included in the application statements or reports or other network management information available from network management systems may also be displayed.

[0104] FIG. 7 is a schematic diagram illustrating another exemplary policy administration console 750 including an authorization dashboard 700 in accordance with various exemplary embodiments of the invention.

[0105] Referring to FIG. 7, the authorization dashboard or controls window 700 may include information fields provisioned and parsed by for example a cloud client (or tenant) 701 and may include users 702, roles 703, authentication realms 704, authentication types 705, instrumented service hosts (or target platforms) 706, service realms 707, identified and attested applications 708, product versions 709 and/or product vendors 710.

[0106] The authorization dashboard 700 for each cloud client 701 may include a plurality of policy components (or rules) for defining a policy (or rule set) for the user 702, a plurality of users, roles 703 or a plurality of roles and an attested application instance 707:708. The dashboard 700 may include administrative controls (not shown) to create filters for perspective views, and issue security alerts based on a plurality of defined criteria and/or provide companion reporting services. The filters may enable, for example, filtering of an authenticated user by an authentication type (or authentication method) 705 for a runtime access control decision. Each row of the illustrated authorization dashboard 700 includes information fields (e.g.,

contents) that may represent (or correspond to) a statement of policy created by the system administrator for the cloud client 701.

[0107] In certain exemplary embodiments, federation of services across different hosting realms may be displayed such that a user authenticated in one authentication domain (or realm) may be provisioned with policy based access to an application hosted in a different target services domain (or realm).

[0108] In certain exemplary embodiments, the attestation broker 102, for example, may be configured to service requests for application artifacts and application statements across a plurality of hosting realms.

[0109] Although the integrity and authorization dashboard is shown with specific information fields and in a particular arrangement, it is contemplated that other information fields and arrangements are possible and that these dashboards may be parsed using any one of the information fields to generate a different perspective view.

[0110] The access control policies created by the system administrator of the cloud client using the authorization dashboard (or console) may be based on runtime context-aware logical attributes pertaining to an attested running application instance such that the contextual information for the attestation may include the runtime local execution context and an introspected security context. There are no physical

constraints wherein rules may require network topology based static attributes, including at least one of: an IPv4/IPv6 address, a port number, a MAC address, a network identifier, a subnet, a VLAN identifier, or combinations or variants thereof.

[0111] Although various embodiments have been described in terms of creating context-aware policies in a cloud environment, it is not limited thereto. The methods may be carried out, for example, between any numbers of computer systems maintaining secure transactions among themselves.

[0112] FIG. 8 is a flowchart illustrating a method 800 in accordance with various exemplary embodiments.

[0113] Referring to FIG. 8, the method 800 may provide an attestation service or broker 109 for an application at runtime executing on a computing platform 101 using an attestation server 109. At block 810, the attestation server 109 remote from the computing platform 101 may receive: (1) a runtime execution context 105 indicating attributes of the application at runtime, and (2) a security context 111 providing security information about the application. At block 820, the attestation server 109 may generate a report 117 indicating security risks associated with the application based on the received runtime execution context 105 and the received security context 111, as an attestation result. At block 830, the attestation server 109 may send the attestation result associated with the application.

[0114] In certain exemplary embodiments, at block 830, the attestation server 109 may also send an automated remediation request to a collaboration service 110 (for example, an orchestration service) to initiate operations on an instrument4ed platform 100 (for example, to reimage, snapshot or quarantine the instrumented platform) based on the attestation result associated with one or more applications (103, 104).

[0115] In certain exemplary embodiments, the attestation server 109 may generate an application artifact 108 as a reference for changes in a subsequent execution context 105 and may send the generated application artifact 108 such that subsequent changes to the runtime execution context 105 are tracked based on the generated application artifact 108.

[0116] In certain exemplary embodiments, the attestation results and the application artifact 108 may be digitally signed.

[0117] In certain exemplary embodiments, the received security context 111 may be an introspective security context and the attestation server 109 may generate one or more security assertions that pertain to the received runtime execution context 105 and the received introspective security context 111.

[0118] In certain exemplary embodiments, a user's transaction with the application may be controlled by applying a set of authorization rules in accordance

with the attestation results. In these and other exemplary embodiments, a user's network access to the application may be controlled based on the set of authorization rules and the attestation results.

[0119] In certain exemplary embodiments, confidence metrics in the attestation results may be provided which indicate a level of security risk by different classifications such that a restriction on a user's transaction with the application may be applied based on the level of security risk indicated by the confidence metrics in the attestation results.

[0120] In certain exemplary embodiments, the restriction on the user's transaction may include the application of routing decisions and the redirection of the user to an alternate computer platform.

[0121] FIG. 9 is a flowchart illustrating a method 900 in accordance with various exemplary embodiments.

[0122] Referring to FIG. 9, the method 900 may provide an attestation service for an application at runtime executing on a computing platform 101 using a runtime monitor 102. At block 910, the runtime monitor 102 at the computing platform 101 may generate a runtime execution context 105 indicating attributes of the application at runtime. At block 920, the runtime monitor 102 may send the runtime execution context 105 to the attestation server 109. At block 930, the runtime monitor may

receive an application artifact 107 for tracking subsequent changes to the runtime execution context 105. At block 940, the runtime monitor 102 using an application artifact 107 may update and may send the runtime execution context 105, as an updated execution context, responsive to the attributes of the application indicating a change.

[0123] In certain exemplary embodiments, the generation of the runtime execution context 105 may include the runtime monitor 102 inspecting running application processes on the computing platform 101 and generating metadata that includes at least a local runtime execution context.

[0124] FIG. 10 is a flowchart illustrating a method 1000 in accordance with various exemplary embodiments.

[0125] Referring to FIG. 10, the method 1000 may provide mutual attestation for first and second interrelated applications 500 and 501 at runtime using an attestation server 502. The first application 500 may run on a first computing platform 530 and the second application 501 may run on a second computing platform 531. At block 1010, the attestation server 502 remote from the first and second computing platforms 530 and 531 may receive a first runtime execution context 506 of the first application 500 indicating attributes of the first application 500 at runtime and a second runtime execution context 504 of the second application 501 indicating

attributes of the second application 501 at runtime. At block 1020, the attestation server 502 may generate: (1) a first report 515 indicating security risks associated with the first application 500 based on the received first runtime execution context 506, as a first attestation result; and (2) a second report 511 indicating security risks associated with the second application 501 based on the received second runtime execution context 504, as a second attestation result. At block 1030, the attestation server 502 may send the first attestation result associated with the first application 500 to the second computing platform 531 and the second attestation result associated with the second application 501 to the first computing platform 530 for mutual attestation.

[0126] In certain exemplary embodiments, a web browser may render an icon indicating that the first attestation result has been sent and responsive to user selection of the icon, may render the attestation result about the first application which is a web application accessed via the web browser.

[0127] In certain exemplary embodiments, the attestation server 502 may generate a first application artifact 507 as a reference for changes in a subsequent execution context of the first application 500 and a second application artifact 505 as a reference for changes in a subsequent execution context of the second application 501; and may send the generated application artifacts 507 and 505 such that

subsequent changes to the first and second runtime execution contexts 506 and 504 may be tracked in the first and second interrelated applications 500 and 501 based on the generated first and second application artifacts 507 and 505, respectively.

[0128] In certain exemplary embodiments, access by a requestor, for example a user 115, to the first application 500 may be controlled based on the first attestation results and independently based on the second attestation results.

[0129] FIG. 11 is a flowchart illustrating a method of providing attestation of a running application in accordance with various exemplary embodiments.

[0130] Referring to FIG. 11, the method 1100 may provide attestation of a running application (e.g., web or non-web applications). At block 1110, the attestation server 402 may register subscriptions for a plurality of subscribers 412 or users 300 for context change notifications 408 of the running application. At block 1120, the attestation service or server 402 may generate assertions about the running application. At block 1130, the attestation service or server 402 may send to the plurality of subscribers 412 or users 300, the assertions of the running application in response to reception of the context change notification 408. The assertions may include at least confidence metrics indicating a level of security risk of the running application.

[0131] FIG. 12 is a flowchart illustrating a method 1200 in accordance with various exemplary embodiments.

[0132] Referring to FIG. 12, the method 1200 may provide mutual attestation of applications in client-server or peer-to-peer transactions using an attestation server. At block 1210, the attestation server 502 may generate (1) a first application artifact 507 for tracking changes in a runtime execution context 506 associated with a client 530 in the client-server transaction, and (2) a second application artifact 505 associated with a server 531 in the client-server transaction. At block 1220, the attestation server 502 may send the first application artifact 507 to the client 530 and the second application artifact 505 to the server 531. At block 1230, the first and second application artifacts 507 and 505 may be exchanged such that the client 530 and the server 531 each have the first and second application artifacts 507 and 505 to mutually track changes in runtime execution contexts 506 and 504 associated with the client 530 and the server 531 for client server transactions.

[0133] Although a client-server transaction between a client and a server is shown, it is contemplated that mutual attestation may be provided by an attestation server between first and second peers or among first, second and/or further peers in a peer-to-peer environment.

[0134] FIG. 13 is a flowchart illustrating a method 1300 in accordance with various exemplary embodiments.

[0135] Referring to FIG. 13, the method 1300 may provide mutual attestation of applications in client-server or peer-to-peer transactions using an attestation server. At block 1310, the attestation server 502 may generate and send a first application artifact 507. At block 1320, the attestation server 502 may receive and validate from a server 531 in the client-server transaction, the first application artifact 507 sent by the attestation server 502 to a client 530 in a client server transaction. At block 1330, the attestation server 502 may generate and send application statements 511 and 515 to the client 530 and the server 531 about interrelated applications 500 and 501 used in the client-server transaction. For example, the sending of the application statements 511 and 515 to the client 530 and the server 531 may include: sending by the attestation server 502: (1) the application statement 511 regarding a client application 500 of the interrelated applications 500:501 to the server 531 of the client-server transaction and the application statement 515 regarding a server application 501 of the interrelated applications 500:501 to the client 530 of the client-server transaction.

[0136] In certain exemplary embodiments, the attestation server 502 may generate and send a second application artifact 505, may receive the second

application artifact 505 from a client 530 in the client server transaction and may validate the second application artifact 505 sent by the attestation server 502 to a server 531 in a client server transaction.

[0137] In certain exemplary embodiments, a method of providing attestation services for applications at runtime may include one or more of the following steps: hosting, by an instrumented target platform, a target user or service program; generating, by an application attestation service: (1) a globally unique, opaque, time-sensitive application artifact; and (2) at least one application statement including a plurality of assertions pertaining to an inspection based runtime local execution context and an introspection based security context; inspecting, by a runtime monitor, running application processes on the instrumented target platform; generating, by the runtime monitor, metadata that includes at least the runtime local execution context; authenticating, by an identity provider, a user to a web application; providing an attestation of the local execution and introspected security context of the web application based on a web services request; controlling, by a network access enforcer, access of an authenticated user to a target application using a subscription based application attestation service; and/or providing, by a collaboration service, the introspected based security context for the target application running on the instrumented target platform.

[0138] In certain exemplary embodiments, a method for providing attestation of the authenticity of a running web application or web servlet may include one or more of the following steps: requesting an application artifact for a running web application or servlet instance; establishing a secure channel between the web server and the attestation server; generating at least one hash file digest corresponding to the execution context of the web application or servlet instance; determining at least one file attribute corresponding to at least one element or the execution context of the web application or web servlet instance; sending an application report to an identity provider; generating assertions based on a received security context and a received local execution context; transmitting confidence metrics in the report to the identity provider; and/or providing attestation of the running web application or web servlet as a digital icon for rendering by a web browser.

[0139] In certain exemplary embodiments, the attestation may be provided prior to (1) commencing any data exchange in an established connection with a user; and/or (2) establishing a network connection with a user.

[0140] In certain exemplary embodiments, the rendering of attestation information about a web application to be accessed may be responsive to user input.

[0141] In certain exemplary embodiments, a system for continuously monitoring running applications hosted on self-managed and on-premise, or on outsourced service provider managed infrastructure may include one or more of the following: an instrumented target platform for hosting a target user or service program; an application attestation service for generating a globally unique, opaque, and time-sensitive application artifact and application statements including a plurality of assertions pertaining to inspection based runtime local execution context and introspection based security context; a runtime monitor for discovering, identifying and inspecting running application processes on the instrumented target platform and for generating metadata that includes at least the runtime local execution context; a collaboration service to provide introspected security context for a target application running on the instrumented target platform; and/or a graphical user interface for: (1) requesting and receiving dynamic assertions from a metadata repository of the attestation service, the dynamic assertions pertaining to the local execution context the introspected security context of running application instances on instrumented target platforms; (2) for continuously displaying the dynamic assertions to a system administrator; and for provisioning and dispatching alerts based on the dynamic assertions and predefined criteria.

[0142] In certain exemplary embodiments, the network access enforcer may subscribe for and receives dynamic application statements from the attestation service to analyze the contextual assertions and to determine whether an authenticated user is permitted or denied network access to an attested application instance.

[0143] In certain exemplary embodiments, the graphical user interface may display the applications running on instrumented target platform on a client specific dashboard or portal, and may present for each associated application execution context at least one of: (1) a service hostname; (2) a service realm; (3) a service principal name; (4) a product version; (5) product vendor; (6) one or more classifications based confidence metrics; or (7) an active network service port.

[0144] In certain exemplary embodiments, the identity provider may query for dynamic application statements from the attestation server to analyze the contextual assertions and to determine whether an authenticated user is permitted or denied authorization to transact data exchanges with an attested application instance in an established connection.

[0145] In certain exemplary embodiments, the network access enforcer may analyze classifications based confidence metrics included in received dynamic application statements, based on a subscription, from the attestation service to

determine whether an authenticated user is permitted or denied network access to an attested application instance.

[0146] In certain exemplary embodiments, the identity provider may analyze classifications based confidence metrics included in received dynamic application statements, based on a subscription, from the attestation service to determine whether an authenticated user is permitted or denied authorization to transact data exchanges with an attested application instance in an established connection.

[0147] In certain exemplary embodiments, a method for creating context-aware policies for network connections or data exchange transactions between authenticated users and attested running applications hosted on self-managed and on-premise, or on outsourced service provider managed infrastructures may include one or more of the following steps: hosting, by an instrumented target platform, a target user or service program; generating, by an application attestation service, a globally unique, opaque, and time-sensitive application artifact and application statements comprising of a plurality of assertions pertaining to inspection based runtime local execution context and introspection based security context; discovering, identifying and inspecting, by a runtime monitor, running application processes on the instrumented target platform generate, by a runtime monitor, metadata that includes at least the runtime local execution context; authenticating,

by an identity provider, a user to a web application based on a web services request to provide attestation of the local execution and introspected security context of the web application; controlling, by a network access enforcer, access of an authenticated user to a target application using the application attestation service that is subscription based; providing, by a collaboration service, an introspected security context for the target application running on the instrumented target platform; and/or creating, using a graphical user interface, access control rules for users annotated by a distinguished name in a user directory or database, and applications annotated by a registered globally unique security principal name.

[0148] In certain exemplary embodiments, context-aware access control policies may be created that stipulate acceptable thresholds for authorizations on the basis of dynamic classifications based confidence metrics.

[0149] Although exemplary embodiments have been described in terms of a computing device or instrumented platform, it is contemplated that it may be implemented in software on microprocessors/general purpose computers such as the computer system 1400 illustrated in FIG. 14. In various embodiments, one or more of the functions of the various components may be implemented in software that controls a computing device, such as computer system 1400, which is described below with reference to FIG. 14.

[0150] Aspects of the present invention shown in FIGS. 1-13, or any part(s) or function(s) thereof, may be implemented using hardware, software modules, firmware, non-transitory computer readable media having instructions stored thereon, or a combination thereof and may be implemented in one or more computer systems or other processing systems.

[0151] FIG. 14 illustrates an example computer system 1400 in which embodiments of the present invention, or portions thereof, may be implemented as computer-readable code. For example, network systems 150, 250, 340, 450 and 550 of FIGS. 1-5, can be implemented in computer system 1400 using hardware, software, firmware, non-transitory computer readable media having instructions stored thereon, or a combination thereof and may be implemented in one or more computer systems or other processing systems. Hardware, software, or any combination of such may embody any of the modules and components used to implement the network systems of FIGS. 1-5.

[0152] If programmable logic is used, such logic may execute on a commercially available processing platform or a special purpose device. One of ordinary skill in the art may appreciate that embodiments of the disclosed subject matter can be practiced with various computer system configurations, including multi-core multiprocessor systems, minicomputers, mainframe computers, computers linked or

clustered with distributed functions, as well as pervasive or miniature computers that may be embedded into virtually any device.

[0153] For instance, at least one processor device and a memory may be used to implement the above described embodiments. A processor device may be a single processor, a plurality of processors, or combinations thereof. Processor devices may have one or more processor "cores."

[0154] Various embodiments of the invention are described in terms of this example computer system 1400. After reading this description, it will become apparent to a person skilled in the relevant art how to implement the invention using other computer systems and/or computer architectures. Although operations may be described as a sequential process, some of the operations may in fact be performed in parallel, concurrently, and/or in a distributed environment, and with program code stored locally or remotely for access by single or multi-processor machines. In addition, in some embodiments the order of operations may be rearranged without departing from the spirit of the disclosed subject matter.

[0155] Processor device 1404 may be a special purpose or a general purpose processor device. As will be appreciated by persons skilled in the relevant art, processor device 1404 may also be a single processor in a multi-core/multiprocessor system, such system operating alone, or in a cluster of computing devices operating

in a cluster or server farm. Processor device 1404 is connected to a communication infrastructure 1406, for example, a bus, message queue, network, or multi-core message-passing scheme.

[0156] Computer system 1400 also includes a main memory 1408, for example, random access memory (RAM), and may also include a secondary memory 1410. Secondary memory 1410 may include, for example, a hard disk drive 1412, removable storage drive 1414. Removable storage drive 1414 may comprise a floppy disk drive, a magnetic tape drive, an optical disk drive, a flash memory, or the like.

[0157] The removable storage drive 1414 reads from and/or writes to a removable storage unit 1418 in a well known manner. Removable storage unit 1418 may comprise a floppy disk, magnetic tape, optical disk, etc. which is read by and written to by removable storage drive 1414. As will be appreciated by persons skilled in the relevant art, removable storage unit 1418 includes a non-transitory computer usable storage medium having stored therein computer software and/or data.

[0158] In alternative implementations, secondary memory 1410 may include other similar means for allowing computer programs or other instructions to be loaded into computer system 1400. Such means may include, for example, a removable storage

unit 1422 and an interface 1420. Examples of such means may include a program cartridge and cartridge interface (such as that found in video game devices), a removable memory chip (such as an EPROM, or PROM) and associated socket, and other removable storage units 1422 and interfaces 1420 which allow software and data to be transferred from the removable storage unit 1422 to computer system 1400.

[0159] Computer system 1400 may also include a communications interface 1424. Communications interface 1424 allows software and data to be transferred between computer system 1400 and external devices. Communications interface 1424 may include a modem, a network interface (such as an Ethernet card), a communications port, a PCMCIA slot and card, or the like. Software and data transferred via communications interface 1424 may be in the form of signals, which may be electronic, electromagnetic, optical, or other signals capable of being received by communications interface 1424. These signals may be provided to communications interface 1424 via a communications path 1426. Communications path 1426 carries signals and may be implemented using wire or cable, fiber optics, a phone line, a cellular phone link, an RF link or other communications channels.

[0160] In this document, the terms “computer program medium,” “non-transitory computer readable medium,” and “computer usable medium” are used to generally

refer to media such as removable storage unit 1418, removable storage unit 1422, and a hard disk installed in hard disk drive 1412. Signals carried over communications path 1426 can also embody the logic described herein. Computer program medium and computer usable medium can also refer to memories, such as main memory 1408 and secondary memory 1410, which can be memory semiconductors (e.g. DRAMs, etc.). These computer program products are means for providing software to computer system 1400.

[0161] Computer programs (also called computer control logic) are stored in main memory 1408 and/or secondary memory 1410. Computer programs may also be received via communications interface 1424. Such computer programs, when executed, enable computer system 1400 to implement the present invention as discussed herein. In particular, the computer programs, when executed, enable processor device 1404 to implement the processes of the present invention, such as the stages in the methods illustrated by the flowcharts 800, 900, 1000, 1100, 1200 and 1300 of FIGS. 8-13, discussed above. Accordingly, such computer programs represent controllers of the computer system 1400. Where the invention is implemented using software, the software may be stored in a computer program product and loaded into computer system 1400 using removable storage drive 1414, interface 1420, and hard disk drive 1412, or communications interface 1424.

[0162] Embodiments of the invention also may be directed to computer program products comprising software stored on any computer useable medium. Such software, when executed in one or more data processing device, causes a data processing device(s) to operate as described herein. Embodiments of the invention employ any computer useable or readable medium. Examples of computer useable mediums include, but are not limited to, primary storage devices (e.g., any type of random access memory), secondary storage devices (e.g., hard drives, floppy disks, CD ROMS, ZIP disks, tapes, magnetic storage devices, and optical storage devices, MEMS, nanotechnological storage device, etc.), and communication mediums (e.g., wired and wireless communications networks, local area networks, wide area networks, intranets, etc.).

[0163] It is to be appreciated that the Detailed Description section, and not the Summary and Abstract sections, is intended to be used to interpret the claims. The Summary and Abstract sections may set forth one or more but not all exemplary embodiments of the present invention as contemplated by the inventor(s), and thus, are not intended to limit the present invention and the appended claims in any way.

[0164] Embodiments of the present invention have been described above with the aid of functional building blocks illustrating the implementation of specified functions and relationships thereof. The boundaries of these functional building blocks have

been arbitrarily defined herein for the convenience of the description. Alternate boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed.

[0165] The foregoing description of the specific embodiments will so fully reveal the general nature of the invention that others can, by applying knowledge within the skill of the art, readily modify and/or adapt for various applications such specific embodiments, without undue experimentation, without departing from the general concept of the present invention. Therefore, such adaptations and modifications are intended to be within the meaning and range of equivalents of the disclosed embodiments, based on the teaching and guidance presented herein. It is to be understood that the phraseology or terminology herein is for the purpose of description and not of limitation, such that the terminology or phraseology of the present specification is to be interpreted by the skilled artisan in light of the teachings and guidance.

[0166] Although the invention is illustrated and described herein with reference to specific embodiments, the invention is not intended to be limited to the details shown. Rather, various modifications may be made in the details within the scope and range equivalents of the claims and without departing from the invention.

What is claimed is:

1. A method of providing an attestation service for an application at runtime executing on a computing platform using an attestation server, comprising:

receiving, by the attestation server remote from the computing platform:

a runtime execution context indicating attributes of the application at runtime; and

a security context providing security information about the application;

generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result; and

sending, by the attestation server, the attestation result associated with the application.

2. The method of claim 1, further comprising:

generating, by the attestation server, an application artifact as a reference for changes in a subsequent execution context; and

sending the generated application artifact such that subsequent changes to the runtime execution context are tracked based on the generated application artifact.

3. The method according to claim 2, further comprising digitally signing the attestation results and the application artifact.

4. The method of claim 1, wherein the received security context is an introspective security context.

5. The method of claim 1, wherein the generating of the report indicating security risks associated with the application includes generating, by the attestation server, one or more security assertions that pertain to the received runtime execution context and the received introspective security context.

6. The method according to claim 1, further comprising authenticating the application using a plurality of collaboration services.

7. The method according to claim 1, further comprising controlling a user's transaction with the application by applying a set of authorization rules in accordance with the attestation results.

8. The method according to claim 1, further comprising controlling a user's network access to the application by applying a set of authorization rules in accordance with the attestation results.

9. The method according to claim 1, further comprising providing confidence metrics in the attestation results indicating a level of security risk by different classifications such that a restriction on a user's transaction with the

application are applied based on the level of security risk indicated by the confidence metrics in the attestation results.

10. The method according to claim 9, wherein the application of the restriction on the user's transaction includes applying the restriction on the user's network access to the application.

11. The method according to claim 1, wherein the application of the restriction on the user's transaction includes applying routing decisions and redirecting the user to an alternate computer platform.

12. The method according to claim 1, further comprising controlling, by a network access enforcer, access of a user to the application based on the attestation result.

13. A non-transitory computer readable medium having instructions stored thereon that, if executed by a computing device, cause the computing device to perform operations for providing mutual attestation of applications in client-server or peer-to-peer transactions using an attestation server, the operations comprising:

generating and sending, by the attestation server, a first application artifact;

receiving and validating, by the attestation server from a server in the client server transaction or from a first peer in the peer-to-peer transaction, the first

application artifact sent by the attestation server to a client in a client server transaction or to a second peer in the peer-to-peer transaction;

generating and sending application statements to the client and the server or the first and second peers about interrelated applications used in the client-server or peer-to-peer transactions.

14. The computer readable medium of claim 13, the operations further comprising:

generating and sending, by the attestation server, a second application artifact;

receiving and validating, by the attestation server from a client in the client server transaction or from a second peer in the peer-to-peer transaction, the second application artifact sent by the attestation server to a server in a client server transaction or to a first peer in the peer-to-peer transaction.

15. The computer readable medium of claim 14, wherein:

the sending of the application statements to the client and the server or the first and second peers comprises the following operations:

sending by the attestation server:

the application statement regarding a client application of the interrelated applications to the server of the client-server transaction and the application statement regarding a server application of the interrelated applications to the client of the client-server transaction; or

the application statement regarding a first peer application of the interrelated applications to the second peer of the peer-to-peer transaction and the application statement regarding a second peer application of the interrelated applications to the first peer of the peer-to-peer transaction; and

determining, based at least in part upon the sent application statements, whether to transact data exchanges with associated applications.

16. The computer readable medium of claim 15, wherein:

the generating of the application statements includes:

including in the application statements confidence metrics and contextual assertions; and

the determining whether to transact data exchanges with the associated applications includes:

comparing respective confidence metrics to a set of rules; and

determining whether to transact data exchange based on the comparison.

17. A method for providing attestation of the authenticity of a running web application or web servlet using an attestation server, comprising:

requesting an application artifact for a running web application or servlet instance;

establishing a secure channel between the web server and the attestation server;

generating at least one hash file digest corresponding to the execution context of the web application or servlet instance;

determining at least one file attribute corresponding to at least one element or the execution context of the web application or web servlet instance;

sending an application report to an identity provider;

generating assertions based on a received security context and a received local execution context;

transmitting confidence metrics in the report to the identity provider; and

providing attestation of the running web application or web servlet as a digital icon for rendering by a web browser.

18. The method according to claim 17, wherein the attestation is provided prior to commencing any data exchange in an established connection with a user.

19. The method according to claim 17, wherein the attestation is provided prior to establishing a network connection with a user.

20. The method according to claim 19, further comprising rendering attestation information about the web application to be accessed responsive to user input.

21. A system for continuously monitoring running applications hosted on self-managed and on-premise, or on outsourced service provider managed infrastructure comprising:

an instrumented target platform for hosting a target user or service program;

an application attestation service for:

generating a globally unique, opaque, and time-sensitive application artifact and application statements including a plurality of assertions pertaining to inspection based runtime local execution context and introspection based security context; and

remediating the instrumented target platform, wherein the remediating includes one or more of: a reimage, a snapshot, or a quarantine of the instrumented target platform;

a runtime monitor for discovering, identifying and inspecting running application processes on the instrumented target platform and for generating metadata that includes at least the runtime local execution context;

a collaboration service configured to:

provide introspected security context for a target application running on the instrumented target platform; and

analyze executable file binaries for the target application running on the instrumented target platform; and

a graphical user interface configured to:

request and receive dynamic assertions from a metadata repository of the attestation service, the dynamic assertions pertaining to the local

execution context the introspected security context of running application instances on instrumented target platforms;

continuously display the dynamic assertions to a system administrator; and

provision and dispatch alerts based on the dynamic assertions and predefined criteria.

22. The system according to claim 21, wherein a network access enforcer subscribes for and receives dynamic application statements from an attestation service to analyze the contextual assertions and determine whether an authenticated user is permitted or denied network access to an attested application instance.

23. The system according to claim 21, wherein the graphical user interface displays the applications running on instrumented target platform on a client specific dashboard or portal, and presents for each associated application execution context at least one of:

a service hostname;

a service realm;

a service principal name;

a product version;

a product vendor;

one or more classifications based confidence metrics;

an active network service port; or

executable file binaries.

24. The system according to claim 21, further comprising an identity provider that queries for dynamic application statements from the attestation server to analyze the contextual assertions and to determine whether an authenticated user is permitted or denied authorization to transact data exchanges with an attested application instance in an established connection.

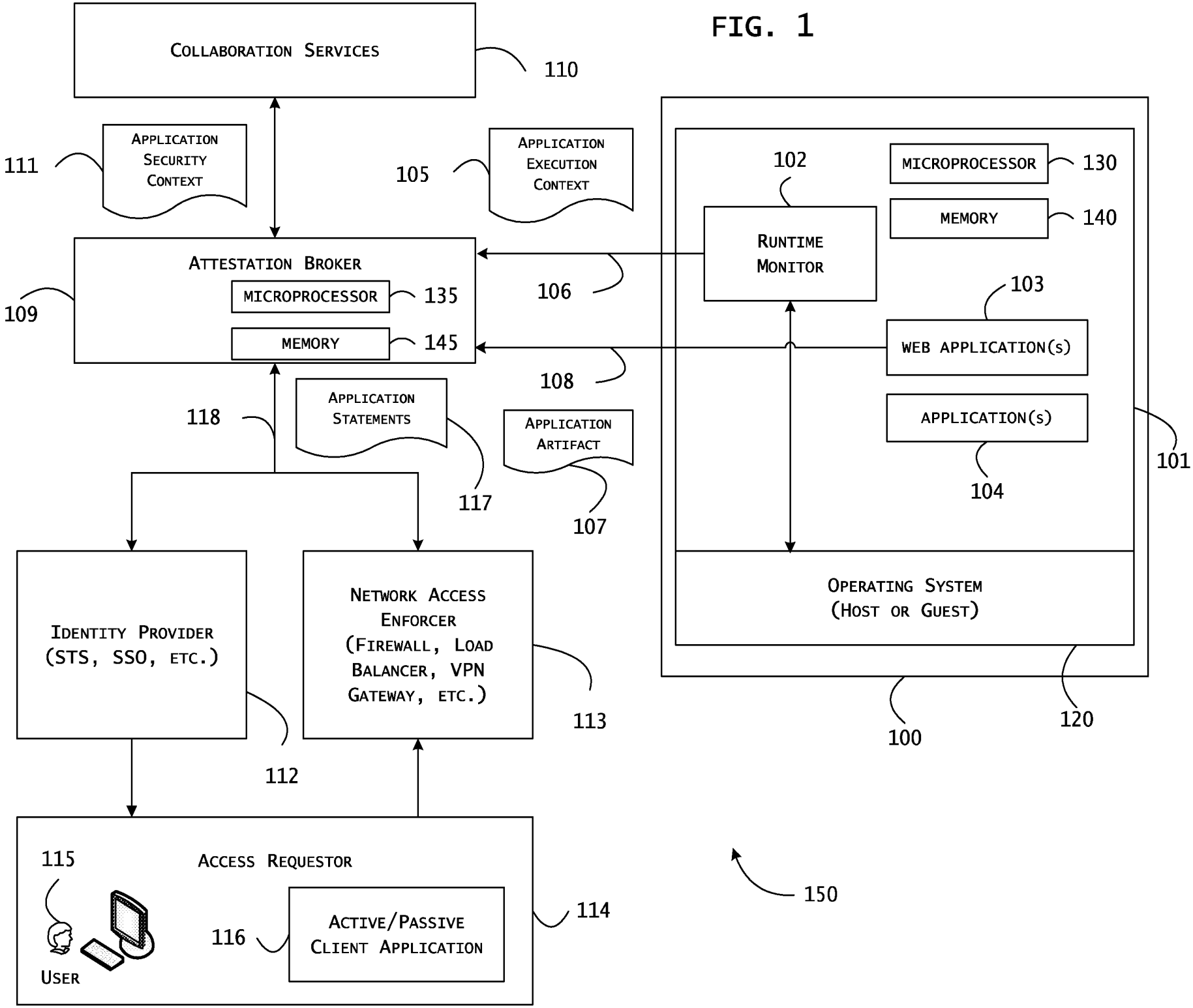
25. The system according to claim 21, further comprising a network access enforcer that analyzes classifications based confidence metrics included in received dynamic application statements, based on a subscription, from an attestation service to determine whether an authenticated user is permitted or denied network access to an attested application instance.

26. The system according to claim 21, wherein an identity provider analyzes classifications based confidence metrics included in received dynamic application statements, based on a subscription, from an attestation service to determine whether an authenticated user is permitted or denied authorization to transact data exchanges with an attested application instance in an established connection.

ABSTRACT OF THE DISCLOSURE

An instrumented machine or platform having a target application thereon is disclosed. An attestation service may generate an application artifact having associated therewith a name and an application statement having at least one of a plurality of attribute value assertions describing the examined runtime local execution and introspection based derived security context. The application statements may represent the level of contextual trustworthiness, at near real time, of a running application on the instrumented target platform. A runtime process and network monitor may examine the local runtime execution context of the target application, and an identity provider may authenticate a user to the web application based on a web services query for attestation of the target application. A physical or logical authorization service may control access of an authenticated user to the target application, based on a dynamic application statement and multi-factor application attestation issued by the attestation service.

FIG. 1



Trend Micro, Inc.
EX1002-225

FIG. 2

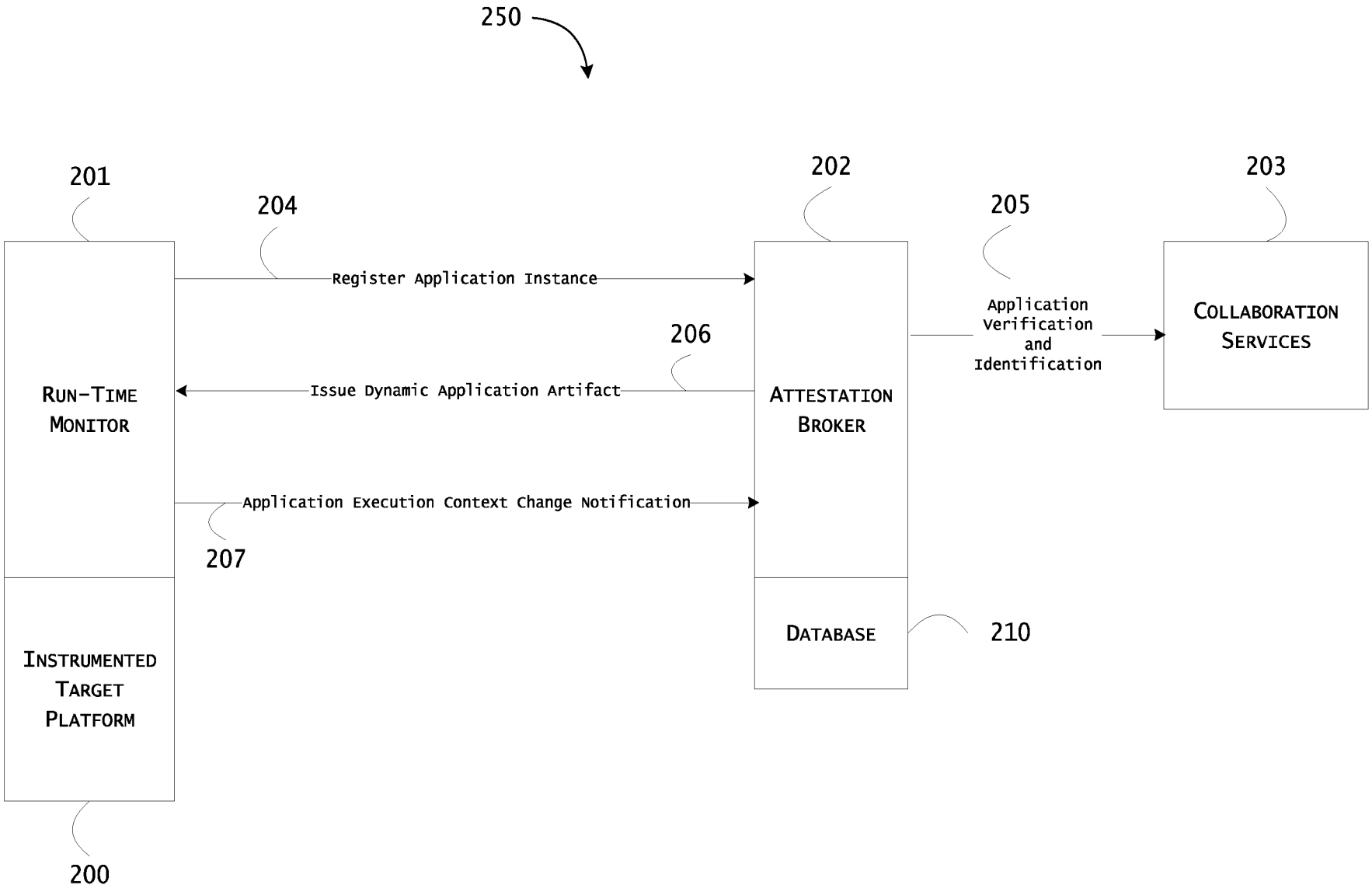

250
201
204
202
205
203
Register Application Instance
Application Verification and Identification
Collaboration Services
206
Run-Time Monitor
Issue Dynamic Application Artifact
Attestation Broker
Application Execution Context Change Notification
207
Database
210
Instrumented Target Platform
200

FIG. 3

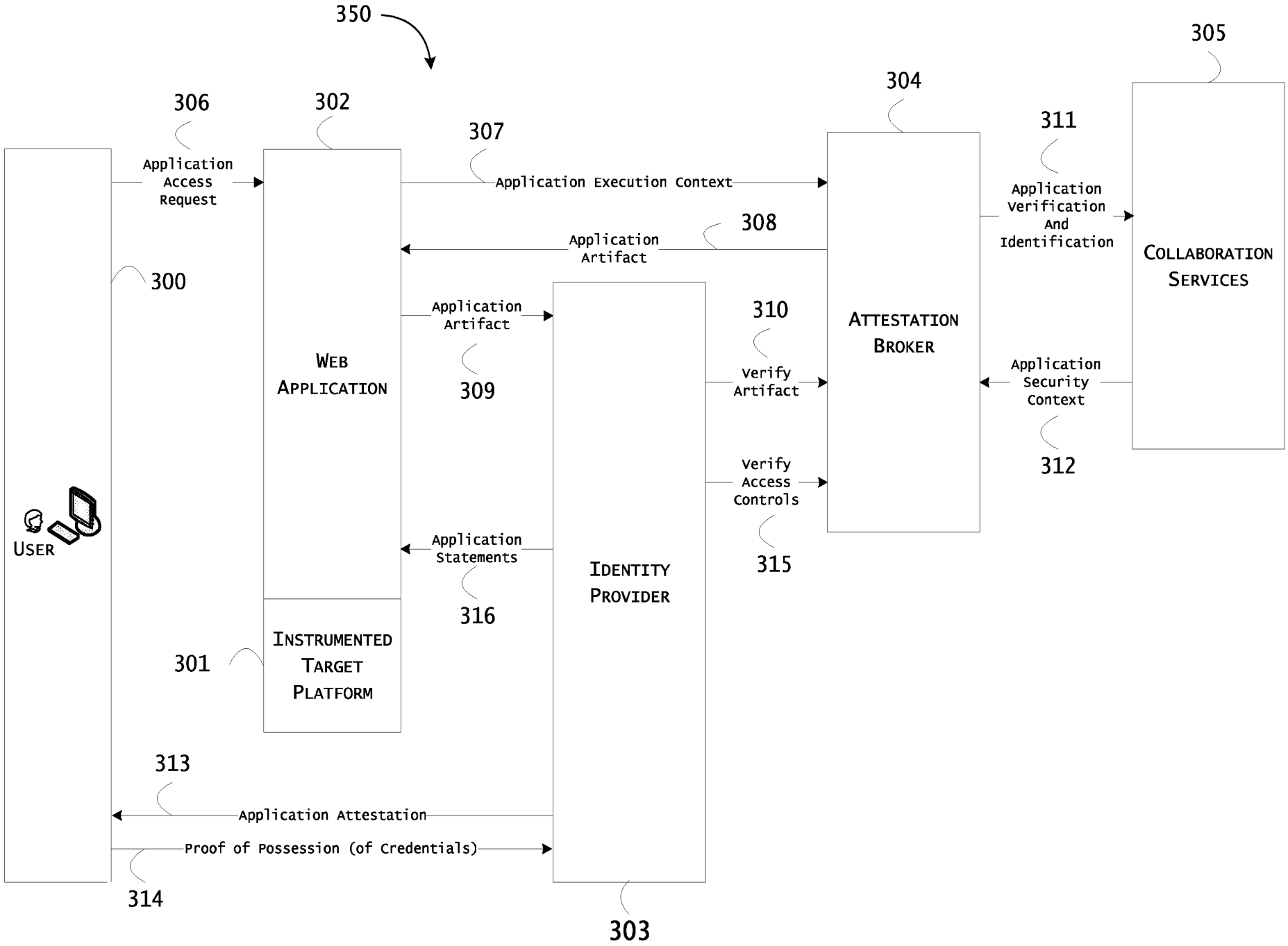
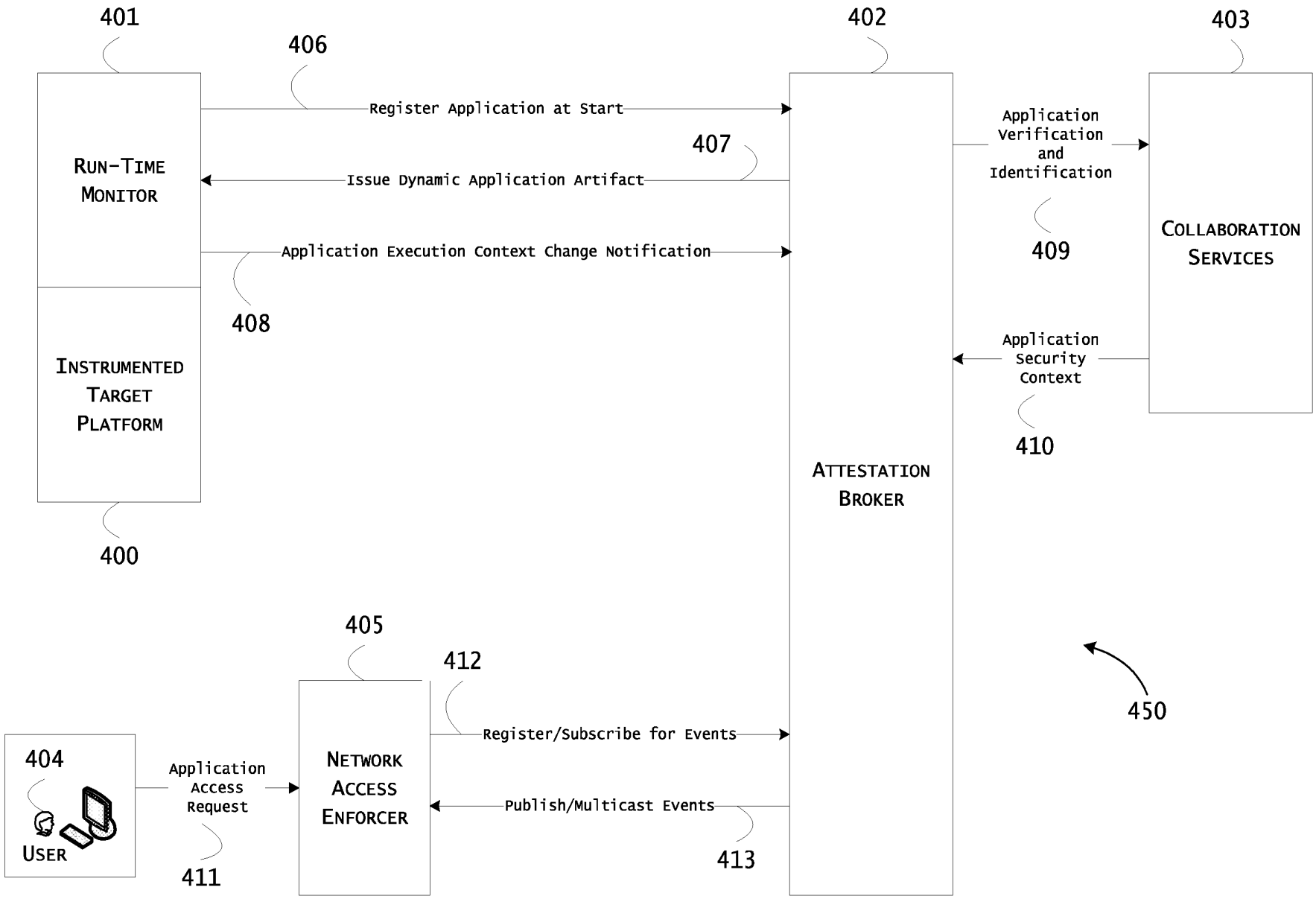
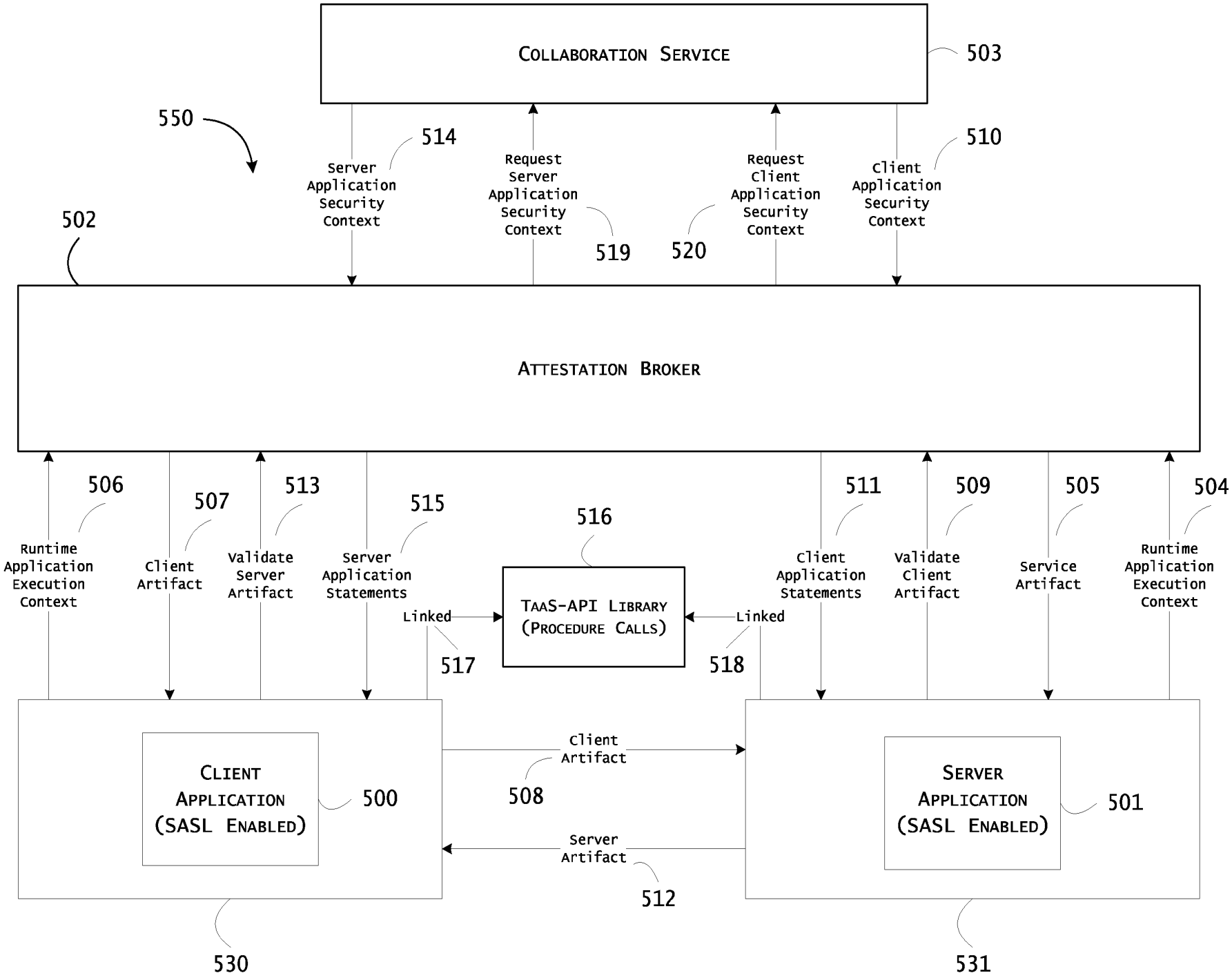

350
306
302
307
304
311
305
Application Access Request
Application Execution Context
Application Verification And Identification
Collaboration Services
308
Application Artifact
300
Web Application
Application Artifact
309
310
Attestation Broker
Verify Artifact
Application Security Context
312
User
Verify Access Controls
315
Application Statements
316
Identity Provider
Instrumented Target Platform
301
313
Application Attestation
Proof of Possession (of Credentials)
314
303

FIG. 4



Trend Micro, Inc.
EX1002-228

FIG. 5



Trend Micro, Inc.
EX1002-229

FIG. 6

650

604 603 602 600 606 605 608 607

TaaS Integrity Dashboard						
Service Host	Service Realm	Service Name	Version	Vendor	Metrics	Ports
ENG0002	eng.dba.com	SharePoint Server	2010	Microsoft Corporation	V/C/R/P	443
DEV0004	dev.eng.dba.com	Apache HTTP Server	2.2	GNU GPL	V/C/R/P	443
QA0005	qa.dba.com	FileZilla Server	0.9.37	GNU GPL	V/C/R/P	21
QA0007	qa.dba.com	Telnet Server	7.0	Microsoft Corporation	V/C/R/P	23
FD0008	finance.dba.com	OpenSSH Server	3.1	GNU GPL	V/C/R/P	22
FD0009	finance.dba.com	IIS Server	3.0	Microsoft Corporation	V/C/R/P	119; 443
TS0010	tech-support.dba.com	Tomcat Server	6.0.29	GNU GPL	V/C/R/P	443
TS0011	tech-support.dba.com	WebSphere Application Server	7.0	IBM	V/C/R/P	443
ELAB0012	lab.qa.dba.com	NetWeaver	7.3	SAP	V/C/R/P	443
ELAB0013	lab.qa.dba.com	WebLogic	10.3.1	Oracle	V/C/R/P	443
PS0014	proserv.dba.com	Microsoft Exchange Server	5.5	Microsoft Corporation	V/C/R/P	379; 443; 445; 993; 995
PM0015	proserv.dba.com	Active Directory	2,000.0	Microsoft Corporation	V/C/R/P	389, 636
BD0016	bizdev.dba.com	Zimbra	10.3.1	VMware, Inc.	V/C/R/P	25; 110; 143; 443
Monitor Date/Time: January 26, 2010 9:18 AM (PST)						

601

FIG. 7

750

700

702	703	704	705	706	707	708	709	710

TaaS Authorization Console

Users	Roles	Auth Realm	Auth Type	Service Host	Service Realm	Service Name	Version	Vendor
Any	Business Development	dba-tp.com	OTP FOB	ENG0003	eng.dba.com	SharePoint Server	2010	Microsoft Corporation
Any	Sales; Support	dbasupplier.com	Password	DEV0004	dev.eng.dba.com	Apache HTTP Server	2.2	GNU GPL
Any	Product Management	dba-tp.com dba-ap.com	Smart Card	QA0005	qa.dba.com	FileZilla Server	0.9.37	GNU GPL
Any	Engineers	dba.com	Password	QA0007	qa.dba.com	Telnet Server	7.0	Microsoft Corporation
ajoe@dba.com asteve@dba.com		dba.com	OTP FOB	FI0008	finance.dba.com	OpenSSH Server	5.1	GNU GPL
Any	QA	dba.com	Password	FI0009	qa.dba.com	IIS Server	5.0	Microsoft Corporation
Any	Server Team	dba.com	Password	TS0010	tech-support.dba.com	Tomcat Server	6.0.29	GNU GPL
Any	Server Team	dba.com	Password	TS0011	tech-support.dba.com	WebSphere Application Server	7.0	IBM
Any	HelpDesk	dba.com	Password	ELAB0012	lab.qa.dba.com	NetWeaver	7.3	SAP
Any	Finance	dba.com	Password	ELAB0013	lab.qa.dba.com	WebLogic	10.3.1	Oracle
Any	Administrators	dba.com	Password	PS0014	proserv.dba.com	Microsoft Exchange Server	5.5	Microsoft Corporation
Any	Administrators	dba.com	OTP FOB	PM0015	proserv.dba.com	Active Directory	2.0/2.0	Microsoft Corporation
Any	Any	dba.com	Password	BD0016	bizdev.dba.com	Zimbra	10.3.1	VMware, Inc.
Any	Staff Engineer	dba.com	OTP FOB	HR0018	hr.dba.net	VisualSVN Server	2.1.4	VisualSVN

Cloud Client: DBA

701

FIG. 8

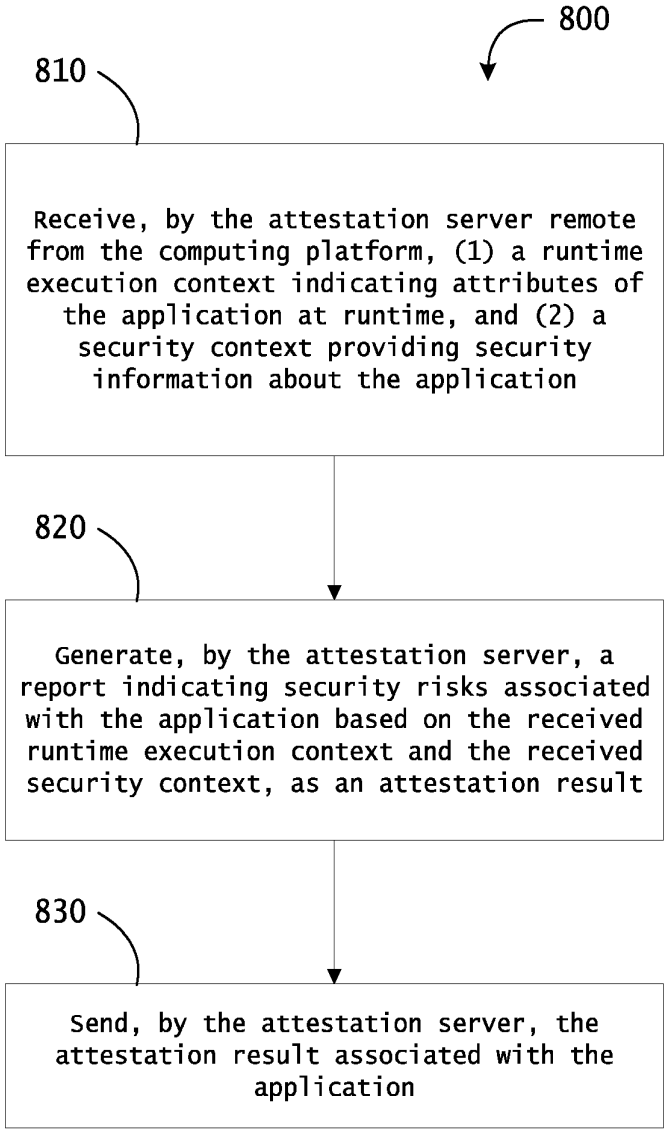
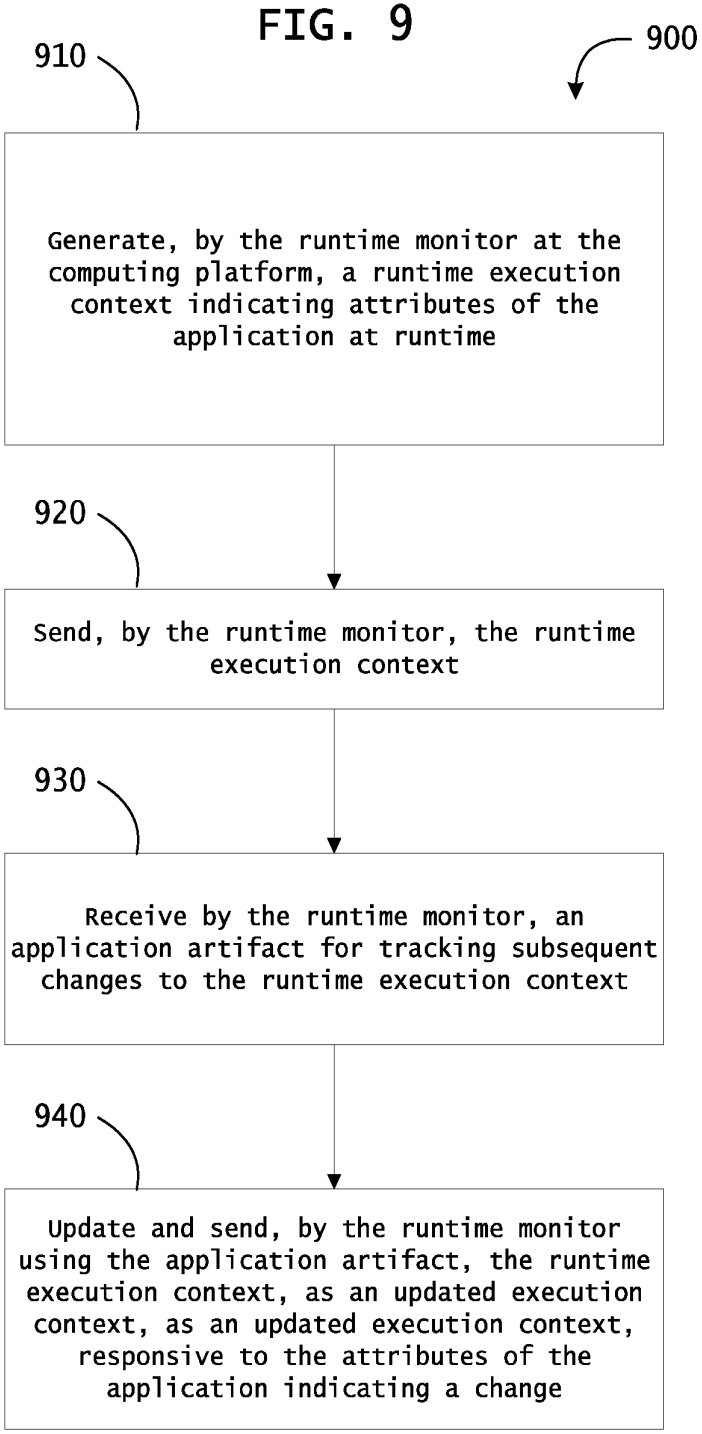


FIG. 9



Trend Micro, Inc.
EX1002-232

FIG. 10

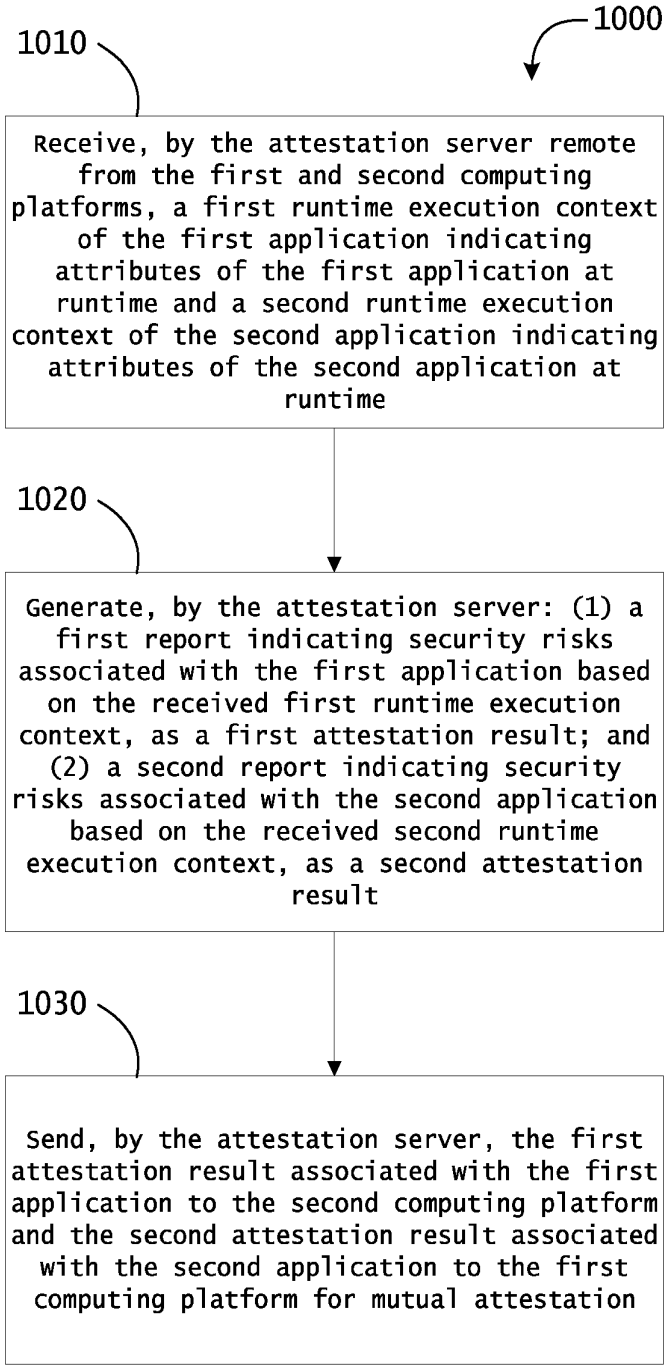

1000
1010
Receive, by the attestation server remote from the first and second computing platforms, a first runtime execution context of the first application indicating attributes of the first application at runtime and a second runtime execution context of the second application indicating attributes of the second application at runtime
1020
Generate, by the attestation server: (1) a first report indicating security risks associated with the first application based on the received first runtime execution context, as a first attestation result; and (2) a second report indicating security risks associated with the second application based on the received second runtime execution context, as a second attestation result
1030
Send, by the attestation server, the first attestation result associated with the first application to the second computing platform and the second attestation result associated with the second application to the first computing platform for mutual attestation

FIG. 11

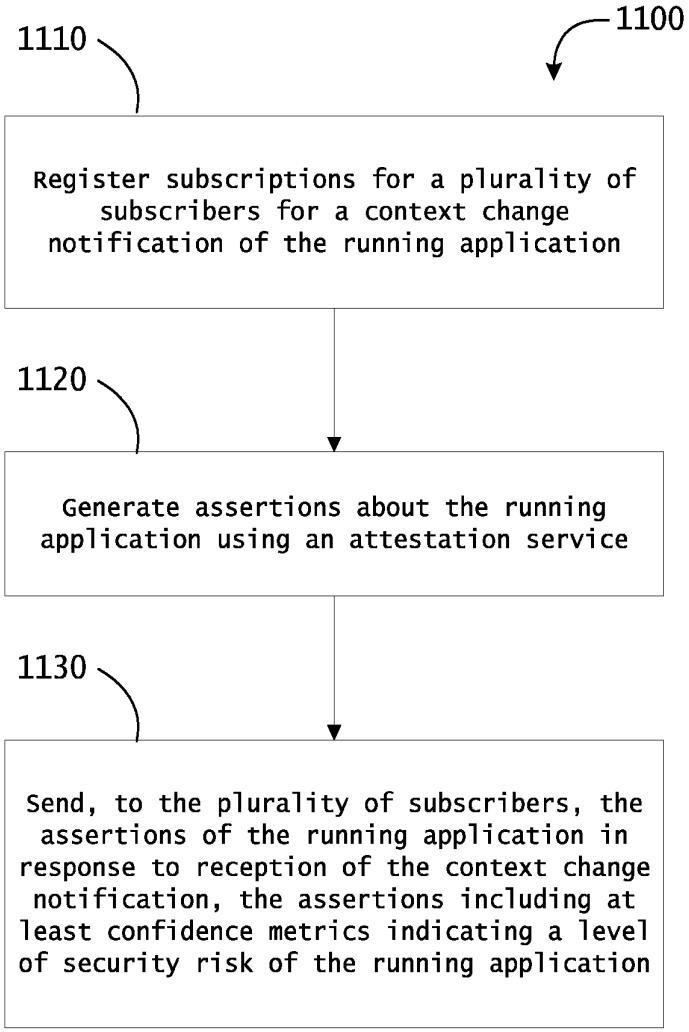

1100
1110
Register subscriptions for a plurality of subscribers for a context change notification of the running application
1120
Generate assertions about the running application using an attestation service
1130
Send, to the plurality of subscribers, the assertions of the running application in response to reception of the context change notification, the assertions including at least confidence metrics indicating a level of security risk of the running application

FIG. 12

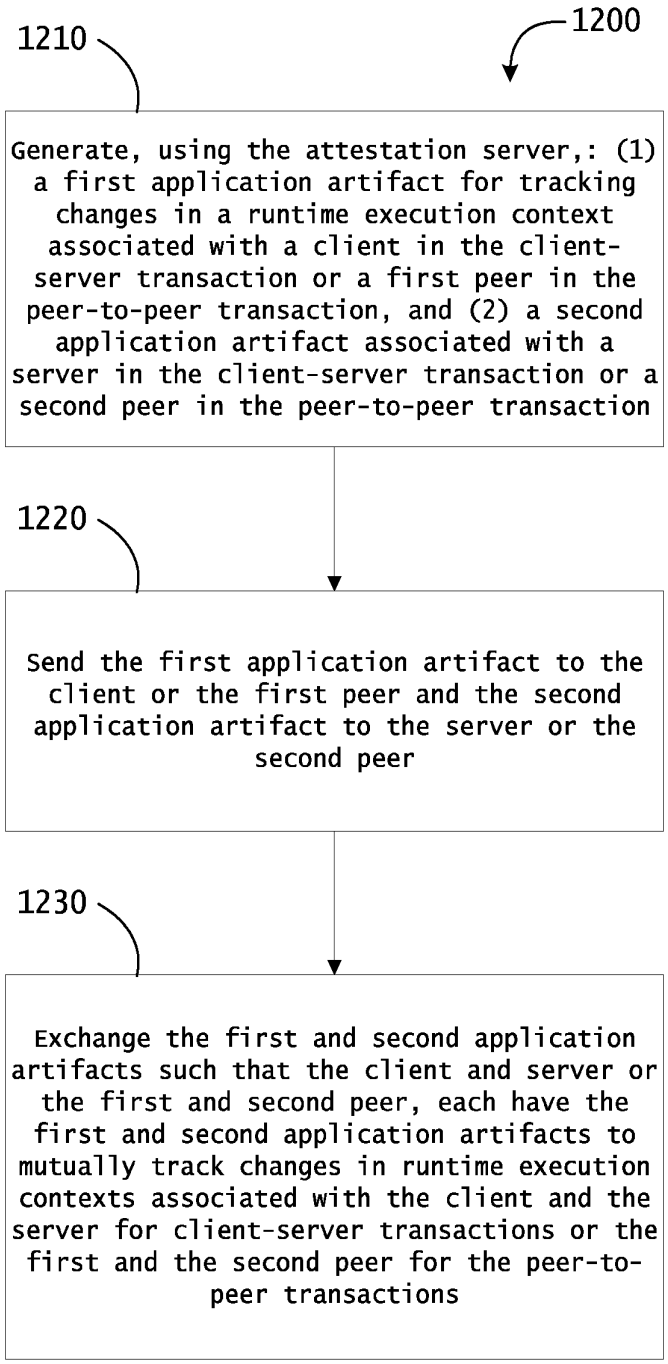

1200
1210
Generate, using the attestation server,: (1) a first application artifact for tracking changes in a runtime execution context associated with a client in the client-server transaction or a first peer in the peer-to-peer transaction, and (2) a second application artifact associated with a server in the client-server transaction or a second peer in the peer-to-peer transaction
1220
Send the first application artifact to the client or the first peer and the second application artifact to the server or the second peer
1230
Exchange the first and second application artifacts such that the client and server or the first and second peer, each have the first and second application artifacts to mutually track changes in runtime execution contexts associated with the client and the server for client-server transactions or the first and the second peer for the peer-to-peer transactions

FIG. 13

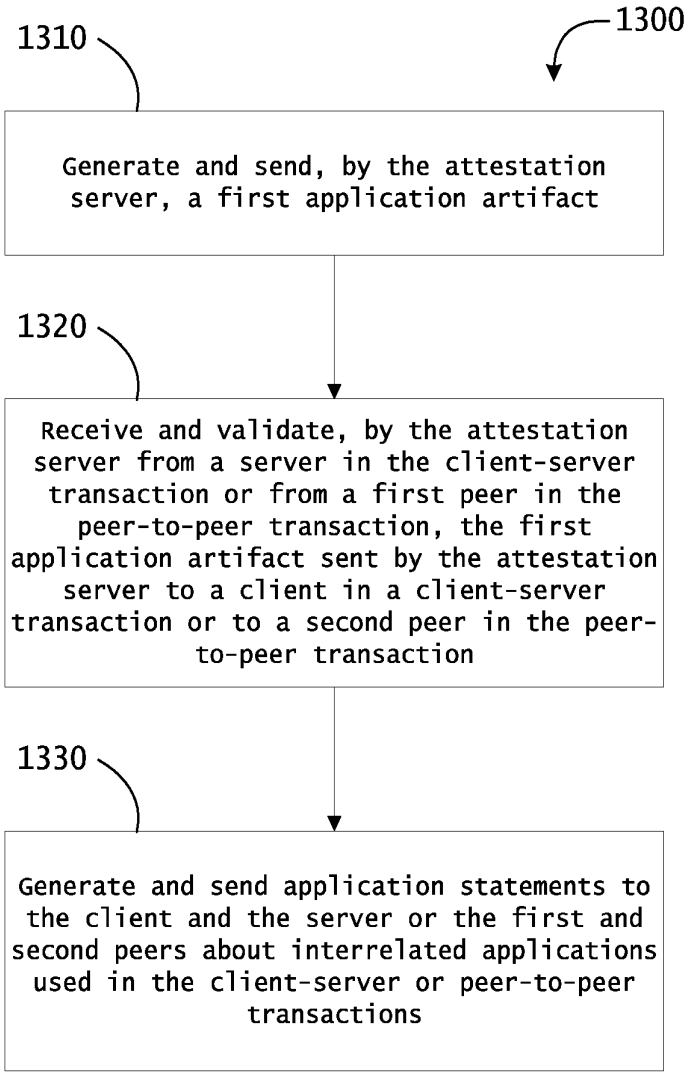
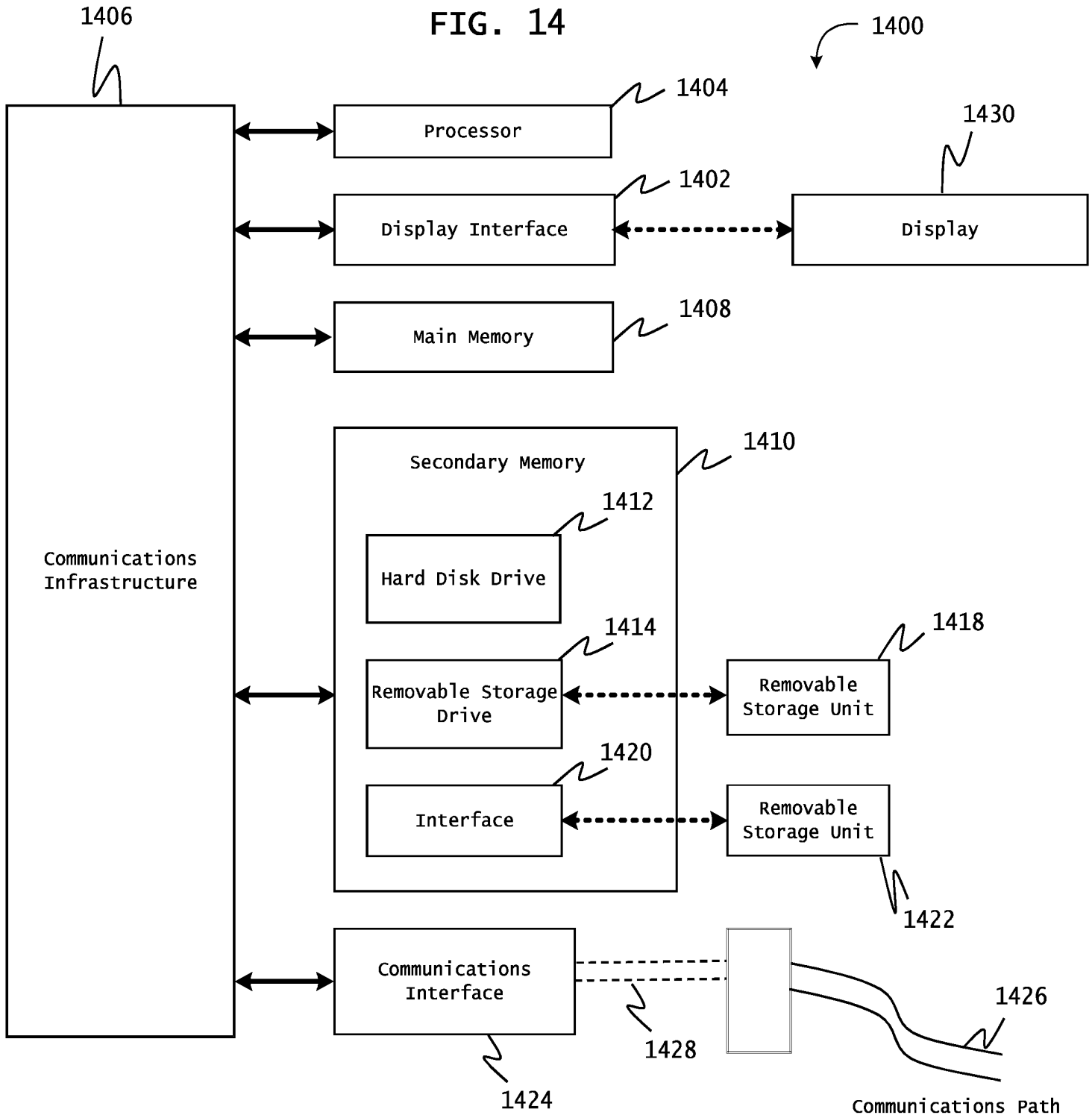

1300
1310
Generate and send, by the attestation server, a first application artifact
1320
Receive and validate, by the attestation server from a server in the client-server transaction or from a first peer in the peer-to-peer transaction, the first application artifact sent by the attestation server to a client in a client-server transaction or to a second peer in the peer-to-peer transaction
1330
Generate and send application statements to the client and the server or the first and second peers about interrelated applications used in the client-server or peer-to-peer transactions

FIG. 14


1400
1406
Communications Infrastructure
1404
Processor
1402
Display Interface
1430
Display
1408
Main Memory
1410
Secondary Memory
1412
Hard Disk Drive
1414
Removable Storage Drive
1418
Removable Storage Unit
1420
Interface
Removable Storage Unit
1422
Communications Interface
1424
1428
1426
Communications Path

PTO/SB/01 (04-09)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)

☑ Declaration Submitted With Initial Filing OR ☐ Declaration Submitted After Initial Filing (surcharge (37 CFR 1.16(f)) required)

Attorney Docket Number	0079152-000002
First Named Inventor	Srinivas KUMAR
COMPLETE IF KNOWN	
Application Number	
Filing Date	
Art Unit	
Examiner Name	

I hereby declare that: (1) Each inventor's residence, mailing address, and citizenship are as stated below next to their name; and (2) I believe the inventor(s) named below to be the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought on the invention titled:

SYSTEM AND METHOD FOR APPLICATION ATTESTATION

(Title of the Invention)

the application of which

☑ is attached hereto

OR

☐ was filed on (MM/DD/YYYY) _____ as United States Application Number or PCT International Application Number _____ and was amended on (MM/DD/YYYY) _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified application, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

Authorization To Permit Access To Application by Participating Offices

☑ If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the above-identified patent application is filed access to the above-identified patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the above-identified patent application is filed to have access to the above-identified patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the above-identified patent application with respect to: 1) the above-identified patent application-as-filed; 2) any foreign application to which the above-identified patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the above-identified patent application; and 3) any U.S. application-as-filed from which benefit is sought in the above-identified patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing the Authorization to Permit Access to Application by Participating Offices.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION — Utility or Design Patent Application

Claim of Foreign Priority Benefits

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? YES	NO
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐

☐ Additional foreign application number(s) are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION — Utility or Design Patent Application

Direct all correspondence to:	☑ The address associated with Customer Number:	21839	OR	☐ Correspondence address below

Name		
Address		
City	State	Zip
Country	Telephone	Email

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1 213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available. Petitioner/applicant is advised that documents which form the record of a patent application (such as the PTO/SB/01) are placed into the Privacy Act system of records DEPARTMENT OF COMMERCE, COMMERCE-PAT-7, System name: *Patent Application Files*. Documents not retained in an application file (such as the PTO-2038) are placed into the Privacy Act system of COMMERCE/PAT-TM-10, System name: *Deposit Accounts and Electronic Funds Transfer Profiles*.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAME OF SOLE OR FIRST INVENTOR:		☐ A petition has been filed for this unsigned inventor	
Given Name (first and middle [if any]) Srinivas		Family Name or Surname KUMAR	
Inventor's Signature Skumar		Date 2/14/2012	
Residence: City Cupertino	State CA	Country USA	Citizenship USA
Mailing Address 10926 Northridge Square			
City Cupertino	State CA	Zip 95014	Country USA

☐ Additional inventors or a legal representative are being named on the 1 supplemental sheet(s) PTO/SB/02A or 02LR attached hereto

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION

ADDITIONAL INVENTOR(S)
Supplemental Sheet

Name of Additional Joint Inventor, if any: ☐ A petition has been filed for this unsigned inventor

Given Name (first and middle (if any))	Family Name or Surname
Gurudatt	SHASHIKUMAR

Inventor's Signature	Date 2/14/2012

Residence: City	State	Country	Citizenship
Foster City	CA	USA	USA

Mailing Address: 618 Plymouth Lane

City	State	Zip	Country
Foster City	CA	94404	USA

Name of Additional Joint Inventor, if any: ☐ A petition has been filed for this unsigned inventor

Given Name (first and middle (if any))	Family Name or Surname

Inventor's Signature	Date

Residence: City	State	Country	Citizenship

Mailing Address

City	State	Zip	Country

Name of Additional Joint Inventor, if any: ☐ A petition has been filed for this unsigned inventor

Given Name (first and middle (if any))	Family Name or Surname

Inventor's Signature	Date

Residence: City	State	Country	Citizenship

Mailing Address

City	State	Zip	Country

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/80 (11-08)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:

☑ Practitioners associated with the Customer Number: 21839

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:

☐ The address associated with Customer Number:

OR

☐ Firm or Individual Name			
Address			
City		State	Zip
Country			
Telephone		Email	

Assignee Name and Address:

TAASERA, INC.
1030 State Street, Erie, Pennsylvania 16501

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature	Kumar	Date	2/16/2012
Name	Srinivas Kumar	Telephone	408-768-4814
Title	Chief Technology Officer		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

SCORE Placeholder Sheet for IFW Content

Application Number: 13399065 Document Date: 2/17/2012

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings – Other than Black and White Line Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions developed by SIRA.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface.
- Other USPTO employees can bookmark the current SCORE URL (http://es/ScoreAccessWeb/).
- External customers may access SCORE content via the Public and Private PAIR interfaces.

Form Revision Date: February 8, 2006