



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.
13/997,412	04/03/2014	Hormuzd M. Khosravi	P41624US/45631-225521	1045
73486	7590	06/09/2017		
Barnes & Thornburg LLP (Intel)			EXAMINER	
11 S. Meridian Street			LE, THANH T	
Indianapolis, IN 46204				
			ART UNIT	PAPER NUMBER
			2495	
			NOTIFICATION DATE	DELIVERY MODE
			06/09/2017	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):

INDocket@btlaw.com
inteldocket@btlaw.com
inteldocs_docketing@cpaglobal.com

Office Action Summary	Application No. 13/997,412	Applicant(s) KHOSRAVI ET AL.	
	Examiner THANH T. LE	Art Unit 2495	AIA (First Inventor to File) Status No

-- 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 MONTHS 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 04/24/2017.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on ____.
- 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) 48-71 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) 48-71 is/are rejected.
- 8) ☐ Claim(s) ____ is/are objected to.
- 9) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

- 10) ☐ The specification is objected to by the Examiner.
- 11) ☐ The drawing(s) filed on ____ 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).

Priority under 35 U.S.C. § 119

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

Certified copies:

- 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)).

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

Attachment(s)

- | | |
|---|---|
| 1) ☒ Notice of References Cited (PTO-892) | 3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____. |
| 2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date <u>01/19/2017 and 04/27/2017</u> . | 4) ☐ Other: ____. |

DETAILED ACTIONS

Notice of Pre-AIA status

1. The present application is being examined under the pre-AIA first to invent provisions.

Information Disclosure Statement

2. The information disclosure statements (IDS) submitted on 01/19/2017 and 04/27/2017 have been considered by the Examiner.

Status of Claims

3. This Office Action is issued in response to the Amendment filed on 04/24/2017.
Claims 1-47 are cancelled.
Claims 48-71 are pending in this Office Action.

Response to Arguments

4. Independent claim 48

Applicant states: "The Office Action indicated that the TPM 44 is the system-on-a-chip. However, contrary to the Office Action's assertions, the TPM 44 does not comprise a security engine that has a secure memory that includes a security key that was encoded in the secure memory during a manufacturing process of the TPM 44 as recite in claim 48. Instead, Kumar discloses in col. 3, 11. 2-7 that "a processing unit key or PUK [of the processing unit 30, and not the TPM 44] is a cryptographic key that is

Art Unit: 2495

stored in a processor when the processor is manufactured, and that remains in the processor in nonvolatile form.”

It seems that the Office Action is asserting that the TPM 44 may be incorporated into the processing unit 30 and function as a single component. However, Kumar states in col. 8, 11. 49-59 that:

[Processing unit 30 and TPM 44 may then use 3PK 72 to create a session key (SK) 74 to be used for protecting communications between processing unit 30 and TPM 44.

Processing unit 30 and TPM 44 may then use SK 74 to create a protected channel, as shown at block 230. That protected channel may traverse multiple system buses 24 and zero or more components of chipset 34. TPM 44 and processing unit 30 may then use SK 74 to encrypt communications, as indicated at block 232. In alternative embodiments, multiple session keys may be used for protecting communications between processing unit 30 and TPM 44.

In other words, the processing unit 30 and the trusted platform module (TPM) 44 are separate components within the same processing system (i.e., within the same computer) that communicates with one another other. As such, the assertion that the processor 22 that includes the processing unit 30 “could also be a secure processor-TPM/system-on-a-chip-with” the processing unit 30 is not supported by Kumar. Accordingly, Kumar fails to disclose or teach at least “a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key that was encoded in the secure

Art Unit: 2495

memory during a manufacturing process of the system-on-a-chip” as recited in claim 48.”

In response, Kumar is brought in to show the obviousness of the limitation “a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip, the session key is encrypted based on the security key and is stored in the secure memory.”

Kumar discloses a system-on-a-chip (Col. 1, lines 26-32: TPM is a system on a chip) comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key (Col. 1, lines 41-46: The sub-components of a TPM may include an execution engine and secure nonvolatile (NV) memory or storage. The secure NV memory is used to store sensitive information, such as encryption keys, and the execution engine protects the sensitive information according to the security policies dictated by the TPM’s control logic). Kumar also discloses “in a platform with a TPM, platform measurements and encryption can be used to seal sensitive information or secrets to the TPM” and in Fig. 1, Processor 22 which has Proc. Unit 30-stores keys and Proc. Unit 32. Therefore, it is obvious to apply TPM to Processor 22 with Proc. Unit 32 as an execution engine and Proc. Unit 30 as secure nonvolatile (NV) memory or storage to protect data of Processor 22.

Applicant states: “Applicant respectfully submits that the Office Action’s assertion that “it is obvious that PKU is also used to encrypt SK to protect SK from attacker” is

Art Unit: 2495

unsupported by Kumar. As quoted above, Kumar discloses in col. 8, lines 49-52 that “processing unit 30 and TPM 44 may then use 3PK 72 to create a session key (SK) 74 to be used for protecting communications between processing unit 30 and TPM 44.” In other words, Kumar teaches that the session key (SK) 74 is created using the third party key (3PK) 72, and that the 3PK may be encrypted based on the PUK. See Kumar, col. 8, 11. 49-52 and col. 2, ln. 67 - col. 3, 11. 1. This is in contrast to encrypting a session key generated from a cryptographic key exchange, wherein the encryption of the session key is performed using a security key that was encoded in the secure memory at the time of manufacture, in accordance with claim 48. As such, Kumar fails to disclose at least that feature of claim 48.”

In response, Kumar teaches the concept of security key is encoded at the time of manufacture (Col. 3, lines 2-7: “a processing unit key or PUK is a cryptographic key that is stored in a processor when the processor is manufactured, and that remains in the processor in nonvolatile form.” Col. 3, lines 9-11: “The platform builder may also install the 3PK into the TPM of the platform during platform manufacturing.”), the concept of encrypting key (Col. 7, lines 44-47: encrypted key is protected from attacker), and the concept of encryption using key that is encoded at the time of manufacture (Col. 6, lines 43-50: PKU is used to encrypt 3KP.) The combination of these concepts makes it obvious to have the encryption of the session key is performed using a security key that was encoded in the secure memory at the time of manufacture.

In conclusion, it is the combination of Kumar’s teachings of TPM, key is encoded at the time of manufacture, and encryption using key that is encoded at the time of

Art Unit: 2495

manufacture that makes the limitation “a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip, the session key is encrypted based on the security key and is stored in the secure memory” obvious. Therefore, Applicant’s arguments regarding Kumar are not persuasive and previous 35 U.S.C. § 103 rejections are maintained.

Applicant’s arguments regarding independent claims 56, 64 and dependent claims 49-55, 57-63, and 65-71 are moot because they depend on Applicant’s arguments of claim 48 which is found non-persuasive.

Claim Rejections - 35 U.S.C. § 103

5. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. **Claims 48-52, 56-61, 64-69 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Chou et al. (US Patent No. 7,966,646), hereinafter "Chou", in view of Asad Mahboob Ali (US Application No. 2006/0041938), hereinafter "Ali" and further in view of Kumar et al. (US Patent No. 8364975), hereinafter "Kumar".**

Regarding claim 48, Chou discloses system-on-a-chip apparatus comprising:

[a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip, the security engine to]:

generate a random nonce for initiating a request for a secure communication session with a [remote] server over a network using the nonce (Fig. 1 and associated text: Client hello message 150 is sent from first network device-client- to second network device-server. Fig. 2A and associated text: Client hello message 150 includes first random number-random nonce. Col. 7, lines 22-23: “the first random number generated by the first network device”);

perform a cryptographic key exchange with the [remote] server (Fig. 1, step 180 and associated text: client key exchange message is sent to second network device-server);

generate a symmetric session key, based on the cryptographic key exchange, to encrypt messages sent to the [remote] server and decrypt messages received from the [remote] server during the secure communication session (Col. 5, lines 63-67: a Master key can be produced prior to completion of the SSL/TLS authentication procedure. The Master key is now used as a symmetric key for supporting encrypted communications between the network devices 110 and 120);

[encrypt the symmetric session key based on the security key]; and

store the encrypted session key in the [secure memory] (Chou does not explicitly disclose about storing the session key; however, in order for using the key to communicate between the two device in a period of time-a session of communication-, it is obvious that the key must be stored), [the system-on-a-chip] to establish the secure communication session with the remote server over the network using the session key (Col. 4, lines 60-63: Client Hello message 150 is a message that provides second network device 120 with information that is used to establish secured communications between network devices 110 and 120. Col. 5, lines 63-67: a Master key can be produced prior to completion of the SSL/TLS authentication procedure. The Master key is now used as a symmetric key for supporting encrypted communications between the network devices 110 and 120).

Chou does not explicitly disclose the secure communication session is with a **remote** server. However, generating session key for secure communication with a remote server is known in the art and Ali's teaching is an example (Paragraph [0039]: "Client applications on the Internet, such as standard web browsers, can connect to the web server on the smart card using HTTPS protocol. The TLS client side implementation allows the smart card to initiate a secure HTTPS connection to a remote web server on the Internet."

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou's invention of establishing a secure communication session with the server over the network using a session key with Ali's invention of secure communication session is with a remote server. The motivation to

Art Unit: 2495

do so would be enable secure communications end-to-end between the resource-constrained device and the remote node as taught by Ali (paragraph [0007]).

Chou and Ali do not explicitly disclose **a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip, the session key is encrypted based on the security key and is stored in the secure memory.**

However, in the field of protecting data, Kumar discloses a system-on-a-chip (Col. 1, lines 26-32: TPM is a system on a chip) comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key (Col. 1, lines 41-46: The sub-components of a TPM may include an execution engine and secure nonvolatile (NV) memory or storage. The secure NV memory is used to store sensitive information, such as encryption keys. Fig. 1: It is obvious that Processor 22 could also be a secure processor-TPM/system-on-a chip- with Proc. Unit 30 is a secure nonvolatile and the Proc. Unit 30 is the execution engine. Col. 2, lines 17-19: In a platform with a TPM, platform measurements and encryption can be used to seal sensitive information or secrets to the TPM) that was encoded in the secure memory during a manufacturing process of the system-on-a-chip (Fig. 1: Proc. Unit 30 has PUK 70. Col. 3, lines 2-7: a processing unit key or PUK is a cryptographic key that is stored in a processor when the processor is manufactured, and that remains in the processor in nonvolatile form), the session key is encrypted

Art Unit: 2495

based on the security key and is stored in the secure memory (Fig. 1: Proc. Unit 30 stores PUK, 3PK, and SK-session key. Col. 6, lines 43-50: PKU is used to encrypt 3KP. Col. 7, lines 44-47: encrypted key is protected from attacker. Therefore, it is obvious that PKU is also used to encrypt SK to protect SK from attacker.)

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou and Ali's invention of establishing a secure communication session with the remote server over the network using a session key with a system on a chip that contains a secure memory to store session key and the session is encrypted using a key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip as taught by Kumar. The motivation to do so would be to protect data and to seal sensitive information or secrets to a secure area as taught by Kumar (Col. 1, line 8 and Col. 2, lines 17-19).

Regarding claim 49, Chou, Ali, and Kumar disclose the system-on-a-chip apparatus of claim 48, wherein the security engine is further to receive a server nonce from the remote server in a response message to the request for the secure communication session, the response message including a server nonce and store the server nonce in the secure memory (Chou, Figs. 1, 2B and associated text: server hello message 160-response message- includes random number 260. Col. 4, lines 43-57: previously required and stored elements are used for second phase of authentication. It is obvious that server nonce is saved for using in second phase authentication. Combining with Kumar's teaching of secure memory as in claim 48 above, it is obvious

Art Unit: 2495

to have the server's nonce stored in the secure memory to protect the nonce from being compromised).

Regarding claim 50, Chou, Ali, and Kumar disclose the system-on-a-chip apparatus of claim 48, wherein the security engine is further to generate a pre-master key, encrypt the pre-master key using the security key of the security engine, and send the encrypted pre-master key to the remote server (Chou, Col. 5, lines 50-61: first network device generates Pre-Master key. Pre-master key is encrypted with the public key of second network device and is sent to second network device-server. Kumar, Col. 3, lines 27-34: 3PKs are used to generate session key. Col. 6, lines 43-50: PKU is used to encrypt 3KP. The combination of Chou and Kumar's teaching makes it obvious that pre-master key is generated and encrypted using the security key of the security engine).

Regarding claim 51, Chou, Ali, and Kumar disclose the system-on-a-chip apparatus of claim 50, wherein the security engine is further to wrap the pre-master key using a server public key and store the wrapped pre-master key in the secure memory (Chou, Col. 5, lines 50-57: first network device generates Pre-Master key and pre-master key is encrypted with the public key of second network device. Kumar, Col. 1, lines 41-46: The secure NV memory is used to store sensitive information, such as encryption keys. Fig. 1: Proc. Unit 30 stores PUK, 3PK, and SK-session key. Col. 6, lines 43-50: PKU is used to encrypt 3KP. Col. 7, lines 44-47: encrypted key is protected from attacker. Therefore, the combination of Chou and Kumar's teachings make it

Art Unit: 2495

obvious that PKU is also used to encrypt pre-master key and store it in the secure memory to protect it from attacker.)

Regarding claim 52, Chou and Kumar disclose the system-on-a-chip apparatus of claim 50. Chou further discloses wherein the security engine is further to:

generate the session key as a function of the pre-master key (Col. 5, lines 61-65: a master key is produced from the pre-master key); and

calculate a hash function as a function of the random nonce generated by the security engine and a nonce received from the remote server (Col. 3, lines 27-29: The completion of a TLS handshake includes a hash of all the frames sent and received by each peer. Col. 7, lines 11-17: According to one embodiment of the invention, each hash value is a result produced by performing one-way hash operations on authentication messages during the SSL/TLS Handshake. These hash operations may be in accordance with MD5, SHA-1 or other hash algorithms that are performed in an iterative to produce a single hash value or in any other selected manner. The hash value is used by the CP processing element to continue the remaining portion of the SSL/TLS Handshake. Therefore, it is obvious that the designer can calculate hash function on his/her choices of values which could be random numbers from client and server).

Claims 56-58 and 64-66 are rejected because they disclose similar subject matter to claims 48-50 respectively.

Claims 59 and 67 are rejected because they disclose similar subject matter to claim 48.

Claims 60-61 and 68-69 are rejected because they disclose similar subject matter to claim 52.

7. **Claims 53, 54, 62, 63, 70, and 71 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Chou et al. (US Patent No. 7,966,646), hereinafter "Chou", in view of Asad Mahboob Ali (US Application No. 2006/0041938), hereinafter "Ali", in view of Kumar et al. (US Patent No. 8364975), hereinafter "Kumar", in view of William Stallings (http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_Security.pdf), hereinafter, "Stallings", and further in view of Jin-Meng Ho (US application No. 2010/0042839), hereinafter "Ho"..**

Regarding claim 53, Chou, Ali, and Kumar disclose the system-on-a-chip apparatus of claim 48. Chou further discloses that client hello message includes list of cryptographic algorithms supported by first network device 110 such as Ephemeral Diffie-Hellman (DHE). Chou also discloses data is encrypted with server's public key before being sent to the server (Chou, Col. 5, lines 50-57: pre-master key is encrypted with the public key of second network device-server).

Chou, Ali, and Kumar do not explicitly disclose wherein the security engine to generate a public Diffie-Hellman client key and a private Diffie-Hellman client key, sign the public Diffie-Hellman client key using a security key of the security engine, and send the signed public Diffie-Hellman key to the remote server.

Art Unit: 2495

However, using Diffie-Hellman public and private keys in handshake process, signing and sending data are well-known in the art and Stallings' teaching is an example (page 540: "Ephemeral Diffie-Hellman: This technique is used to create ephemeral (temporary, one-time) secret keys. In this case, the Diffie-Hellman public keys are exchanged, signed using the sender's private RSA or DSS key. The receiver can use the corresponding public key to verify the signature. Certificates are used to authenticate the public keys. This would appear to be the most secure of the three Diffie-Hellman options because it results in a temporary, authenticated key.")

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou, Ali, and Kumar's inventions of establishing a secure communication session with remote server over the network using a session key with a system on a chip that contains a secure memory to store sensitive information and with Stallings' invention of using Diffie-Hellman keys, signing and sending data. The motivation to do so would be to provide authentication.

Chou, Ali, Kumar and Stallings do not explicitly disclose that the security engine **generate** the Diffie-Hellman keys itself. However, generating Diffie-Hellman keys by sender is known in the art and Ho's teaching is an example ((Fig. 3, step 0a and associated text: a secret (private) key is chosen and a public key is computed. Paragraph [0038]: public key generated initiating device A-client- is used for Diffie-Hellman key exchange).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou, Ali, Kumar and Stallings' inventions

Art Unit: 2495

of establishing a secure communication session with remote server over the network using a session key with a system on a chip that contains a secure memory to store sensitive information with using Diffie-Hellman keys, signing and sending data and with Ho's invention of generating Diffie-Hellman keys by sender. The motivation to do so would be to allow two parties to exchange information over an insecure channel to establish a shared secret as taught by Ho (paragraph [0022]).

Regarding claim 54, Chou, Ali, Kumar, Stallings and Ho disclose the system-on-a-chip apparatus of claim 53. Ho further discloses wherein the security engine to receive a public Diffie-Hellman server key from the server (Fig. 3, step 4b and associated text: Public key of device B-server- is sent to device A) and generate the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key (step 5a and associated text: DHkey-session key- is computed based on Private key of device A –client- and public key of Device B-server).

Art Unit: 2495

8. Claims 53, 54, 62, 63, 70, and 71 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Chou et al. (US Patent No. 7,966,646), hereinafter "Chou", in view of Asad Mahboob Ali (US Application No. 2006/0041938), hereinafter "Ali", in view of Kumar et al. (US Patent No. 8364975), hereinafter "Kumar", in view of William Stallings (http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_Security.pdf), hereinafter, "Stallings".

Regarding claim 55, Chou, Ali and Kumar disclose the system-on-a-chip apparatus of claim 48. Kumar also discloses the secure memory stores cryptographic key as stated in claim 48.

Chou, Ali and Kumar do not explicitly disclose wherein the security engine to receive Diffie-Hellman global values and a public Diffie-Hellman server key from the server.

However, receiving Diffie-Hellman global values and a public Diffie-Hellman server key from the server are well-known in the art and Stallings' teaching is an example (page 541: "Anonymous Diffie-Hellman: The message content consists of the two global Diffie-Hellman values (a prime number and a primitive root of that number) plus the server's public Diffie-Hellman key.")

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou, Ali, and Kumar's inventions of establishing a secure communication session with remote server over the network using

Art Unit: 2495

a session key with a system on a chip that contains a secure memory to store sensitive information and with Stallings' invention of receiving Diffie-Hellman global values and a public Diffie-Hellman server key from the server. The motivation to do so would be to provide web security for client and server.

Regarding claim 63, Chou, Ali, and Kumar disclose the method of claim 56 (claim 56 is rejected for disclosing similar subject matter to claim 48, as stated in section 9 above). Chou further disclose:

generating, in the security engine of the system-on-a-chip, a hash code of a preceding message sent from the client to the server (Col. 3, lines 27-29: The completion of a TLS handshake includes a hash of all the frames sent and received by each peer. Col. 7, lines 11-17: According to one embodiment of the invention, each hash value is a result produced by performing one-way hash operations on authentication messages during the SSL/TLS Handshake. These hash operations may be in accordance with MD5, SHA-1 or other hash algorithms that are performed in an iterative to produce a single hash value or in any other selected manner. The hash value is used by the CP processing element to continue the remaining portion of the SSL/TLS Handshake. Therefore, it is obvious that the designer can calculate hash function on his/her choices of values which could be random numbers from client and server).

Chou, Ali, and Kumar do not explicitly disclose signing the hash code using a security key stored in a secure memory of the security engine and sending a client certificate verification message to the server, the client certificate verification message

Art Unit: 2495

including the signed hash code. However, signing hash code and sending a client certificate verification message are well-known in the art and Stallings' teaching is an example (page 540: "Ephemeral Diffie-Hellman: This technique is used to create ephemeral (temporary, one-time) secret keys. In this case, the Diffie-Hellman public keys are exchanged, signed using the sender's private RSA or DSS key. The receiver can use the corresponding public key to verify the signature. Certificates are used to authenticate the public keys. This would appear to be the most secure of the three Diffie-Hellman options because it results in a temporary, authenticated key." Page 542: "the client may send a certificate_verify message to provide explicit verification of a client certificate... This message signs a hash code based on the preceding messages, defined as follows:

```
CertificateVerify.signature.md5_hash
MD5(master_secret || pad_2 || MD5(handshake_messages ||
master_secret || pad_1));
Certificate.signature.sha_hash
SHA(master_secret || pad_2 || SHA(handshake_messages ||
master_secret || pad_1));)
```

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou, Ali, and Kumar's inventions of establishing a secure communication session with remote server over the network using a session key with a system on a chip that contains a secure memory to store sensitive information and with Stallings' invention of signing and sending signed data. The motivation to do so would be to provide authentication and to ensure secure communication for involved parties.

Art Unit: 2495

Claims 62 and 70 are rejected because they disclose similar subject matter to the combination of claims 53 and 54.

Claim 71 is rejected because it discloses similar subject matter to claim 63.

Conclusion

9. THIS ACTION IS MADE FINAL.

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to THANH T. LE whose telephone number is (571)270-0279. The examiner can normally be reached on M-Th 8:30 am- 2:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Farid Homayounmehr can be reached on 571-272-3739. The fax phone

Art Unit: 2495

number for the organization where this application or proceeding is assigned is 571-273-8300.

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.

/THANH T. LE/

Examiner, Art Unit 2495

/FARID HOMAYOUNMEHR/

Supervisory Patent Examiner, Art Unit 2495