

CERTIFICATION OF MICRO ENTITY STATUS (INSTITUTION OF HIGHER EDUCATION BASIS)					
Application Number or Control Number (if applicable): TBD			Patent Number (if applicable):		
First Named Inventor: Paulo Shakarian, et al.			Title of Invention: SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION		
CERTIFICATION ON THE BASIS OF EMPLOYMENT BY AN INSTITUTION OF HIGHER EDUCATION The applicant hereby certifies the following— The applicant qualifies as a small entity as defined in 37 CFR 1.27. The applicant's employer, from which the applicant obtains the majority of the applicant's income, is an institution of higher education as defined in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a)).					
SIGNATURE by an <u>authorized party</u> set forth in 37 CFR 1.33(b)					
Signature		/Ari M. Bai/			
Name		Ari M. Bai			
Date		November 28, 2016	Telephone	602-650-2000	Registration No. 38726
☐	There is more than one inventor and I am one of the inventors who are jointly identified as the applicant. The required additional certification form(s) signed by the other joint inventor(s) are included with this form.				
CERTIFICATION ON THE BASIS OF ASSIGNMENT OR OBLIGATION TO ASSIGN TO AN INSTITUTION OF HIGHER EDUCATION The applicant hereby certifies the following— The applicant qualifies as a small entity as defined in 37 CFR 1.27. The applicant has assigned, granted, conveyed, or is under an obligation by contract or law, to assign, grant, or convey, a license or other ownership interest in the particular application to an institution of higher education as defined in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a)).					
SIGNATURE by an <u>authorized party</u> set forth in 37 CFR 1.33(b)					
Signature		/Ari M. Bai/			
Name		Ari M. Bai			
Date		November 28, 2016	Telephone	602-650-2000	Registration No. 38726
☐	There is more than one inventor and I am one of the inventors who are jointly identified as the applicant. The required additional certification form(s) signed by the other joint inventor(s) are included with this form.				

NOTE: A signed copy of this "institution of higher education basis" micro entity certification form (PTO/SB/15B) filed together with a signed copy of the "gross income basis" micro entity certification form (PTO/SB/15A) will be taken to be a representation that any inventor or person applying for a patent as provided in 37 CFR 1.46 not qualifying on the "gross income basis" qualifies on the "institution of higher education basis."

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.

Electronic Patent Application Fee Transmittal

Application Number:				
Filing Date:				
Title of Invention:	SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION			
First Named Inventor/Applicant Name:	Paulo Shakarian			
Filer:	Ari M. Bai/Janelle Wiggins			
Attorney Docket Number:	055743-555439			
Filed as Micro Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
BASIC UTILITY PATENT FILING FEE-MCRO-ENT	3011	1	70	70
UTILITY SEARCH FEE	3111	1	150	150
UTILITY EXAMINATION FEE	3311	1	180	180
Pages:				
Claims:				
Miscellaneous-Filing:				
LATE FILING FEE FOR OATH OR DECLARATION	3051	1	35	35
Petition:				

IPR2025-01397

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				435

Electronic Acknowledgement Receipt

EFS ID:	27629350
Application Number:	15362730
International Application Number:	
Confirmation Number:	5936
Title of Invention:	SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION
First Named Inventor/Applicant Name:	Paulo Shakarian
Customer Number:	27148
Filer:	Ari M. Bai/Janelle Wiggins
Filer Authorized By:	Ari M. Bai
Attorney Docket Number:	055743-555439
Receipt Date:	28-NOV-2016
Filing Date:	
Time Stamp:	20:58:00
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	\$435
RAM confirmation Number	112916INTEFSW00007516501662
Deposit Account	
Authorized User	

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

IPR2025-01397

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	055743-555439-ADS.pdf	1823190	no	9
			c9d5092ad182677fcfad7d47cf9ca54dcde22b9f		
Warnings:					
Information:					
2		055743-555439-Specification.pdf	386414	yes	25
			6d80a3d9eaa40556ed08e3146c02566642a4f32a		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	20	
	Claims		21	24	
	Abstract		25	25	
Warnings:					
Information:					
3	Drawings-only black and white line drawings	055743-555439-Drawings.pdf	580991	no	9
			8edb3692fe69bd633f5e4d61283cee096c91bbfd		
Warnings:					
Information:					
4	Certification of Micro Entity (Education Basis)	055743-555439-Cert-Micro-Entity-Status_final.pdf	97121	no	2
			6ab2e36168152884f8ee4dbb031e86d08ebd2f1		
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	36703	no	2
			4356b180ed529ad59cf45054c049ec2856941703		
IPR2025-01307					

IPR2025-01397

Warnings:	
Information:	
Total Files Size (in bytes):	2924419
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.	

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.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	055743-555439
		Application Number	
Title of Invention	SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION		
The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76. This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.			

Secrecy Order 37 CFR 5.2:

☐	Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)
--------------------------	---

Inventor Information:

Inventor	1				Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Paulo		Shakarian		
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					
City	Chandler	State/Province	AZ	Country of Residence	US

Mailing Address of Inventor:

Address 1	3932 West Rene Drive				
Address 2					
City	Chandler	State/Province	AZ		
Postal Code	85226	Country	US		

Inventor	2				Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	John		Robertson		
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					
City	Prescott	State/Province	AZ	Country of Residence	US

Mailing Address of Inventor:

Address 1	3170 Shalom Drive				
Address 2					
City	Prescott	State/Province	AZ		
Postal Code	86301	Country	US		

Inventor	3				Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Jana		Shakarian		
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					

IPR2025-01397

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	055743-555439
		Application Number	
Title of Invention	SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION		

City	Chandler	State/Province	AZ	Country of Residence	US
------	----------	----------------	----	----------------------	----

Mailing Address of Inventor:

Address 1	3932 West Rene Drive				
Address 2					
City	Chandler	State/Province	AZ		
Postal Code	85226	Country	US		
Inventor	4				Remove
Legal Name					

Prefix	Given Name	Middle Name	Family Name	Suffix	
	Vivin		Paliath		
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					
City	Chandler	State/Province	AZ	Country of Residence	US

Mailing Address of Inventor:

Address 1	3960 South Pearl Drive				
Address 2					
City	Chandler	State/Province	AZ		
Postal Code	85249	Country	US		
Inventor	5				Remove
Legal Name					

Prefix	Given Name	Middle Name	Family Name	Suffix	
	Amanda		Thart		
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					
City	Scottsdale	State/Province	AZ	Country of Residence	US

Mailing Address of Inventor:

Address 1	7602 East Aster Drive				
Address 2					
City	Scottsdale	State/Province	AZ		
Postal Code	85260	Country	US		
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button. Add					

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).	
☐	An Address is being provided for the correspondence information of this application. IPR-2025-01397

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	055743-555439	
		Application Number		
Title of Invention	SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION			
Customer Number	27148			
Email Address	uspt@polsinelli.com		Add Email	Remove Email

Application Information:

Title of the Invention	SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION			
Attorney Docket Number	055743-555439	Small Entity Status Claimed	☒	
Application Type	Nonprovisional			
Subject Matter	Utility			
Total Number of Drawing Sheets (if any)	9	Suggested Figure for Publication (if any)		

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐ Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.			
Please Select One:	☒ Customer Number	☐ US Patent Practitioner	☐ Limited Recognition (37 CFR 11.9)
Customer Number	27148		

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	055743-555439
		Application Number	
Title of Invention	SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending	Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Claims benefit of provisional	62261200	2015-11-30
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.			Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)ⁱ the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

			Remove
Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	Access Code ⁱ (if applicable)
Additional Foreign Priority Data may be generated within this form by selecting the Add button.			Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013. NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	055743-555439
		Application Number	
Title of Invention	SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION		

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is 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 State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	055743-555439
		Application Number	
Title of Invention	SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION		

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant	1	Remove
If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section. Clear		
Assignee	Legal Representative under 35 U.S.C. 117	Joint Inventor
☐ Person to whom the inventor is obligated to assign.		☐ Person who shows sufficient proprietary interest
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:		
Name of the Deceased or Legally Incapacitated Inventor:		
If the Applicant is an Organization check here. ☒		
Organization Name	ARIZONA BOARD OF REGENTS ON BEHALF OF ARIZONA STATE UNIVERSITY	
Mailing Address Information For Applicant:		
Address 1	699 South Mills Avenue	
Address 2	Suite 601, Room 691AA	
City	Tempe	State/Province
Country	US	Postal Code
Phone Number		Fax Number
Email Address		
Additional Applicant Data may be generated within this form by selecting the Add button. Add		

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	055743-555439
		Application Number	
Title of Invention	SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION		

Assignee	1			
Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.				
				Remove
If the Assignee or Non-Applicant Assignee is an Organization check here.				☐
Prefix	Given Name	Middle Name	Family Name	Suffix
Mailing Address Information For Assignee including Non-Applicant Assignee:				
Address 1				
Address 2				
City		State/Province		
Country ⁱ		Postal Code		
Phone Number		Fax Number		
Email Address				
Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.				Add

Signature:

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). However, if this Application Data Sheet is submitted with the **INITIAL** filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Ari M. Bai/		Date (YYYY-MM-DD)	2016-11-28
First Name	Ari M.	Last Name	Bai	Registration Number
				38726
Additional Signature may be generated within this form by selecting the Add button.				Add

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	055743-555439
	Application Number	
Title of Invention	SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION	

This collection of information is required by 37 CFR 1.76. 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 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet 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 records.
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.

**UNITED STATES NON-PROVISIONAL PATENT APPLICATION
FOR
SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC
CYBER THREAT MITIGATION**

Inventors:

Paulo Shakarian (USA)

John Robertson (USA)

Jana Shakarian (USA)

Vivin Paliath (USA)

Amanda Thart

Priority:

62/261,200 filed on November 30, 2015

Status:

Micro-Entity

Prepared by:

Polsinelli PC

One East Washington Street, Suite 1200

Phoenix, Arizona

Attorney's Docket No.:

055743-555439

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This is a non-provisional application that claims benefit to U.S. provisional application serial number 62/261,200 filed on November 30, 2015, which is herein incorporated by reference in its entirety.

FIELD

[0002] The present disclosure relates to a security game framework, and in particular to a data-driven security game framework that models an attacker based on exploit market data actively mined from the “darknet” or other overlay communication networks to develop strategies for the defender.

BACKGROUND

[0003] Many corporations rely on extensive penetration testing to assess the security of their computer networks. In a penetration test, a red team is hired to expose major flaws in the firm’s security infrastructure. Recently, however, the market for exploit kits has continued to evolve and what was once a rather hard-to-penetrate and exclusive market — whose buyers were primarily western governments -- has now become more accessible to a much wider population. Specifically, the darknet or other overlay network portions of the Internet accessible through anonymization protocols (such as Tor and i2p) have become populated with a variety of markets specializing in such products. In particular, 2015 saw the introduction of darknet markets specializing in zero-day exploit kits — exploits designed to leverage previously undiscovered vulnerabilities. These exploit kits are difficult and time-consuming to develop — and often are sold at premium prices. A survey of 8 marketplaces shows the price ranges of exploit kits for common software in Table 1 — these prices range from 0.0126-8.4 Bit-coin (2.88-1919.06 U.S. dollars at the time of this writing).

[0004] The widespread availability of zero-day exploits in the darknet represents a potential game changer for penetration testers — specifically posing the following questions:

- What exploits will an attacker likely purchase if he targets my organization?
- What software used in the organization pose the biggest risk to new threats?

[0005] Unfortunately, the high cost of a variety of exploits available through the darknet may preclude a penetration tester from obtaining such exploits at a reasonable price to perform an effective penetration testing that accurately accesses the security of a computer network being tested. While criminal activity on the darknet has been extensively studied over the past decade for issues such as drug trade and terrorism, the markets for exploits existing on the darknet are much less well-understood.

Product	Price in BTC	Price in \$*
GovRAT (Source Code + 1 Code Signing Certificate Included)	2.000	\$456.93
Qday Wordpress MU Remote Shell	1.500	\$342.69
A5/I Encryption Rainbow Tables	1.500	\$342.69
Unlimited Code Signing Certificate	1.200	\$274.16
Ready-made Linux botnet 600 SERVERS	1.200	\$274.16
FUD version of Adobe Flash <= 16.0.0.287 (CVE 2015-0311)	1414.68	\$500.00

*Price in U.S. Dollar as of Sep. 1, 2015 [1 BTC = \$228.46]

Table 1: Example of Products offered on Darknet Markets

[0006] There has been related work on malicious hacker forums which did not focus on the purchase and sale of specific items. Markets of malicious products relevant to cyber security have been previously studied, but none of these works gathered data on specific exploits (or other products) from either the darkweb or open Internet; nor did they examine the markets through the lens of security games.

[0007] In recent years, “security games” where attacker-defender models are used to inform the actions of defenders in military, law-enforcement, and homeland security applications have gained much traction. With regard to cyber-security, there have been many contributions including intrusion detection, attack graph based games, and honey-pot placement. However, there does not appear to be a game theoretic approach to host-based defense where the activities of the attacker are informed from an “un-conventional” source (information not directly related to the defender’s system) - specifically information from darknet markets in this case. Further, the very recent emergence of darknet markets specializing in zero-day exploits allow for the integration of information that was previously

unknown.

BRIEF DESCRIPTION OF THE DRAWINGS

- [0008] FIG. 1 is a schematic of a real-time exploit analysis system;
- [0009] FIG. 2 is a graph showing the distribution of Exploits with respect to platform;
- [0010] FIG. 3A is a graph showing DHAP Payoff vs. Budget for a Windows server and FIG. 3B is a graph showing the DHAP Payoff vs. Budget for a Linux server;
- [0011] FIG. 4A is a graph showing Defender Best Response, Payoff vs. k_{atk} for Windows server and FIG. 4B is a graph showing Defender Best Response, Payoff vs. k_{atk} for Linux server;
- [0012] FIG. 5 is a simplified block diagram illustrating one embodiment of a game-theoretic framework;
- [0013] FIG. 6 is a simplified block diagram of a computer system; and
- [0014] FIG. 7 is a flowchart of a method for applying a game theoretic cyber threat mitigation to a network.
- [0015] Corresponding reference characters indicate corresponding elements among the view of the drawings. The headings used in the figures do not limit the scope of the claims.

DETAILED DESCRIPTION

[0016] Given a system configuration (or a distribution of system configurations within an organization), the present disclosure models an attacker who, given a budget, will purchase exploits to maximize his level of access to the target system. Likewise, a defender will look to adjust system configurations in an effort to minimize the effectiveness of an attacker while ensuring that necessary software dependencies are satisfied.

[0017] The present system introduces a rigorous and thoroughly analyzed framework for addressing penetration testing that is fed with real-world exploit market data, mined from the darknet. FIG. 1 provides a schematic diagram 100 of our framework. In one embodiment, a new security game framework 100 is designed to model an attacker with access to exploit markets and a defender of information technology infrastructure; theoretical analysis of the framework leading to the development of algorithms to find near-optimal strategies for both players; and an implementation of the system and the results of a thorough suite of experiments on real-world data.

[0018] In some embodiments, the framework 100 includes a security game where the attacker 102 is a malicious hacker with access to a darknet exploit markets 104 and the defender 106 is tasked with host-based defense of either a single or group of systems. The notation V is used herein to represent the entire set of vulnerabilities within a given computer system. Though there may be vulnerabilities not yet detected by the system administrator, information on new vulnerabilities can be mined through an examination of darknet hacking markets. In a real-world organization, system administrators are not able to patch all vulnerabilities for a variety of reasons. Software dependencies, use of legacy systems, and non-availability of patches are some examples. To model this, a “constraint set” (denoted C) is defined as a subset of V . The vulnerabilities in a constraint set represent the vulnerabilities required for some system functionality. When each vulnerability in a constraint set C is in the presented attack surface (i.e. externally accessible), C is then said to be satisfied and the system supports the functionality modeled by C .

[0019] In particular, let C represent the set of all possible constraint sets. This idea is extended with an “application constraint set” which, for an arbitrary

application, i , denoted C_i , is a set of constraint sets (i.e. $C_i \subseteq C$). Each constraint set in C_i represents a set of vulnerabilities that together will provide complete functionality of application i . C_i is said to be satisfied if any single constraint set in C_i is satisfied. If C_i is satisfied by a system configuration, and hence at least one constraint set in C_i is satisfied, application i will properly operate on the system. C is the set of all application constraint sets for a given system configuration and represents all of the applications to be run on the system. So, in this framework, for a given system, a system administrator selects which vulnerabilities may be present in order to allow each application i to function. This begs the question as to how to make this selection. As such, the process is begun by defining some concepts relevant to the adversary.

[0020] The term ex is used to denote a particular exploit - a technique used to take advantage of a given vulnerability. Let Ex denote the set of all possible exploits and Ex denote the set of all possible exploit sets (i.e. $Ex = 2^{Ex}$). For each $ex \in Ex$, c_{ex} is the associated cost of exploit ex - and this is specified directly on a darknet market 104 (normally in Bitcoin). Associated with the set of exploits is the Exploit Function, ExF , which takes a set of exploits as input and returns a set of vulnerabilities (i.e. $ExF : \mathbf{Ex} \rightarrow 2^V$). The set of vulnerabilities produced by $ExF(A)$, for a given set of exploits A , represents the vulnerabilities that are exploited by the exploits in A . While many possible variations of an exploit function are possible, in this paper, we will use a straightforward definition that extends the exploit function from singletons (whose associated vulnerabilities can be taken directly from the online marketplaces) to sets of exploits: $ExF(A) = \bigcup_{a \in A} ExF(\{a\})$. For use in proving complexity results, we shall denote the special case where $Ex = V$, $ExF(A) = A$, and $\forall ex \in Ex, c_{ex} = 1$ as the “Identity Exploit Model”.

[0021] Player Strategies and Payoff. An attacker 102 will use a set of exploits to attempt to gain access to a system, and will do so within a budget. Likewise, the defender 106 identifies a set of vulnerabilities that he is willing to expose (often referred to as the “presented attack surface”). Strategies for the two players formally defined as follows.

[0022] Definition 2.1. (Attack Strategy). Given budget $k_{atk} \in \mathbb{R}^+$, an *Attack Strategy*, denoted A is a subset of Ex s.t. $\sum_{a \in A} c_a \leq k_{atk}$.

[0023] Definition 2.2. (Defense Strategy). Given a family of application constraint sets $C = \{C_0, C_1, \dots, C_n\}$, a *Defense Strategy*, denoted D is a subset of V

s.t. for each $C_i \in C$, there exists $C \in C_i$ where $C \subseteq D$.

[0024] Note that when a defense strategy D meets the requirements of C , as per Definition 2.2, we say D satisfies C . We will use the notation $\mathbf{A}, \mathbf{D}$ to denote the set of all attack and defense strategies, respectively, and refer to an attacker-defender pair of strategies as a “strategy profile.” We will also define a *mixed strategy* for both players in the normal manner. For the attacker (resp. defender) a mixed strategy is a probability distribution over $\mathbf{A}$ (resp. $\mathbf{D}$). Mixed strategies as Pr_A, Pr_D are normally denoted for each player and use the notation $|Pr_A|$ (resp. $|Pr_D|$) to denote the number of strategies in $\mathbf{A}$ (resp. $\mathbf{D}$) that are assigned a nonzero probability by the mixed strategy. The payoff function may be defined formally as follows:

[0025] Definition 2.3. (Payoff Function). A payoff function, p , is any function that takes a strategy profile as an argument and returns a positive real. Formally, $p : \mathbf{A} \times \mathbf{D} \rightarrow \mathbb{R}^+$

[0026] Unless noted otherwise, the payoff function will be treated as being computable in polynomial time. Also, the payoff function is underspecified - which is designed to allow flexibility in the framework. The following “payoff function axioms” are contemplated:

$$\forall D \in \mathbf{D}, \forall A \in \mathbf{A} \text{ s.t. } \text{Exp}(A) \cap D = \emptyset, p(A, D) = 0 \quad (1)$$

$$\forall D \in \mathbf{D}, \forall D' \subseteq D, \forall A \in \mathbf{A}, p(A, D') \leq p(A, D) \quad (2)$$

$$\forall D \in \mathbf{D}, \forall A \in \mathbf{A}, \forall A' \subseteq A, p(A', D) \leq p(A, D) \quad (3)$$

$$\forall A \in \mathbf{A}, D, D' \in \mathbf{D}, p(A, D) + p(A, D') \geq p(A, D \cup D') \quad (4)$$

$$\forall D \in \mathbf{D}, A, A' \in \mathbf{A}, p(A, D) + p(A', D) \geq p(A \cup A', D) \quad (5)$$

[0027] Axiom 1 states that if the vulnerabilities generated by an attack strategy's exploits and the vulnerabilities in a defense strategy are disjoint sets, the payoff function must return 0. A consequence of axiom 1 is that if either the attack strategy or the defense strategy is the empty set, the payoff function will return 0. Axioms 2 and 3 require the payoff function to be monotonic in the size of the attack and defense strategies. Axioms 4 and 5 require the payoff function to be sub-modular with respect to the attack and defense strategies.

[0028] The present disclosure focuses on the “over-lap payoff function” which is defined as follows: $p(A, D) = |\text{Exp}(A) \cap D|$. Intuitively, this is simply the number of vulnerabilities exploited by the attacker. Further, when dealing with mixed strategies, payoff in terms of expectation will be discussed. Expected payoff can be

formally defined as follows:

$$Exp(Pr_A, Pr_D) = \sum_{D \in \mathbf{D}} \sum_{A \in \mathbf{A}} Pr_A(A) Pr_D(D) p(A, D)$$

[0029] Using the overlap function, the expected payoff can be interpreted as the “expected number of exploited vulnerabilities.”

[0030] **Best Response Problems.** A pair of decision problems dealing with the best response for the players will now be described below. These problems are the deterministic host attacker problem (DHAP) and deterministic host defender problem (DHDP), respectively, and are defined as follows:

DHAP.

[0031] INPUT: $k_{atk} \in \mathbb{R}^+$, $x \in \mathbb{R}^+$, mixed defense strategy Pr_D , and payoff function p .

[0032] OUTPUT: “Yes” if $\exists A \in \mathbf{A}$ s.t. $\sum_{a \in A} c_a \leq k_{atk}$ and $\sum_{D \in \mathbf{D}} Pr_D(D) p(A, D) \geq x$, “No” otherwise.

DHDP.

[0033] INPUT: $x \in \mathbb{R}^+$, application constraints C , mixed attack strategy Pr_A , and payoff function p .

[0034] OUTPUT: “Yes” if $\exists D \in \mathbf{D}$ s.t. $\sum_{A \in \mathbf{A}} Pr_A(A) p(A, D) \leq x$ and D satisfies C . and “No” otherwise.

[0035] The natural optimization variants for these two problems will deal with maximizing the payoff in DHAP and minimizing the payoff in DHDP.

Analysis and Algorithms

[0036] The complexity and limits of approximation for both DHAP and DHDP will now be analyzed. The “Identity Exploit Model” is used for the complexity results. Unfortunately, both problems are NP-Complete in the general case.

[0037] **Theorem 1.** DHAP is NP-Complete, even when $|Pr_D|$ and the payoff function adheres to the submodularity and monotonicity axioms.

[0038] *Proof Sketch.* Membership in NP is trivial if the payoff is PTIME computable. The hardness result relies on an embedding of the well-known budgeted set cover. Here, the defender’s strategy is treated as a set of elements to cover and the exploits are treated as subsets of D (by virtue of the exploit function). Exploit costs are set as 1 and the attacker’s budget is the value budget from the embedded problem. So, the attacker must pick exploits to meet the budget and

cover the determined number of the defender's vulnerabilities.0

[0039] Theorem 2. When $|C| > 1$ and $|Pr_A| = 1$, DHDP is NP-Complete.

[0040] Proof Sketch. Again, membership in NP is trivial if the payoff is PTIME computable. Hardness is shown by embedding the hitting set problem. In this reduction, the attacker plays all exploits and each exploit corresponds with precisely one vulnerability. This has the effect of imposing a unit cost on each vulnerability. Here, each C_i must be covered by a vulnerability. Hence, the defender must pick a set of all vulnerabilities to meet the cost requirement of DHDP while covering each C_i .

[0041] The hardness of approximation is also analyzed for the optimization variants of DHAP and DHDP. Due to the fact that the above embeddings used set cover and hitting set, we can draw upon the known past results to obtain the following corollaries:

[0042] Corollary 3. DHAP cannot be approximated where the payoff is within a factor of $(1 - \frac{1}{e})$ unless $P = NP$

[0043] Corollary 4. DHDP cannot be approximated where the payoff is within a factor of $(1 - o(1)) \ln(n)$ unless $P = NP$

[0044] With the limits of approximation in mind, several algorithms are introduced to solve the optimization variants of DHAP and DHDP. The optimization variant of DHAP under the overlap payoff function is a special case of sub-modular maximization with the distinction that we are not simply picking k discrete objects, but instead picking items that each have a unique cost associated with them. Understanding this, several different approaches are examined to this problem based on the literature on submodular maximization. DHDP, on the other hand, can be readily approximated using the traditional set-cover algorithm (under some realistic assumptions), as cost does not affect DHDP.

Algorithm 1 Lazy Greedy Algorithm (Cost-Benefit Variant)

Input: $k_{atk} \in \mathbb{R}^+$, Pr_D , and payoff function p .

Output: $A \subseteq Ex$ s.t. $\sum_{a \in A} c_a \leq k_{atk}$

```
1:  $A \leftarrow \emptyset$ ;  $cost \leftarrow 0$ ; priority queue  $Q \leftarrow \emptyset$ ;  $iteration \leftarrow 1$ 
2: for  $e \in Ex$  do
3:    $e.key \leftarrow \frac{\Delta_{Pr_D}(e|\emptyset)}{c_e}$ ;  $e.i \leftarrow 1$ 
4:   insert  $e$  into  $Q$  with “key” as the key
5: end for
6: while  $\{a \in Ex \setminus A : c_a + cost \leq k_{atk}\} \neq \emptyset$  do
7:   extract top (max) element  $e$  of  $Q$ 
8:   if  $e.i = iteration$  then
9:      $A \leftarrow A \cup \{e\}$ ;  $iteration \leftarrow iteration + 1$ 
10:     $cost \leftarrow cost + c_e$ 
11:   else
12:     $e.i \leftarrow iteration$ ;  $e.key \leftarrow \frac{\Delta_{Pr_D}(e|A)}{c_e}$ ;
13:    re-insert  $e$  into  $Q$ 
14:   end if
15: end while
16: return  $A$ 
```

Algorithms for DHAP

[0045] Greedy Approaches. As mentioned earlier, the non-unit cost of exploits mean that DHAP can be considered as a submodular maximization problem subject to knapsack constraints. Two versions of the traditional greedy algorithm can be applied: a cost-benefit variant and uniform-cost variant, both of which will also use the lazy-greedy optimization to further enhance performance while maintaining the approximation guarantee. It was independently noted that the uniform-cost and the cost-benefit algorithms can perform arbitrarily badly. However, by extending a result from either the cost-benefit or the uniform-cost algorithm will provide a solution within a factor of $\frac{1}{2}(1 - 1/e)$ for a given set of input parameters. By applying both algorithms to a given problem instance and returning the attack strategy which produces the larger payoff, the $\frac{1}{2}(1 - 1/e)$ approximation factor is achieved for DHAP. A cost-benefit lazy approximation algorithm is shown in Algorithm 1. By removing “ ce ” from the denominator in the $e.key$ assignment in lines 3 and 12, the cost benefit lazy approximation algorithm is transformed into a uniform cost lazy approximation algorithm.

[0046] Multiplicative Update Approach. An improved approximation ratio, when compared with the $\frac{1}{2}(1 - 1/e)$ ratio for the greedy algorithms, can be obtained by adapting Algorithm 1 for DHAP. This is shown as Algorithm 2 in this disclosure. For some value ϵ (a parameter), this algorithm provides a $(1 - \epsilon)(1 - 1/e)$

approximation of the optimal solution (Theorem 1.2), which, by providing an exceedingly small ϵ value, can get arbitrarily close to the $\frac{1}{2}(1 - 1/e)$ optimal approximation limit we discussed earlier.

Algorithm 2 Multiplicative Update

Input: $k_{atk}, \epsilon \in \mathbb{R}^+$ s.t. $0 < \epsilon \leq 1$, Pr_D , and payoff function p .

Output: $A \subseteq Ex$ s.t. $\sum_{a \in A} c_a \leq k_{atk}$

```

1:  $Ex' \leftarrow \{ex \in Ex : c_{ex} \leq k_{atk}\}$ 
2:  $A \leftarrow \emptyset$ 
3:  $W \leftarrow \min_{ex'_i \in Ex'} k_{atk}^2 / c_{ex'_i}$ 
4:  $w \leftarrow 1/k_{atk}; \lambda \leftarrow e^{eW/4}$ 
5: while  $k_{atk}w \leq \lambda$  and  $Ex' \neq \emptyset$  do
6:    $ex_j \leftarrow \operatorname{argmin}_{ex_j \in Ex' \setminus A} \frac{c_{ex_j}}{k_{atk}} w / \Delta_{Pr, Pr_D}(ex_j | A)$ 
7:    $A \leftarrow A \cup \{ex_j\}$ 
8:    $w \leftarrow w \lambda^{c_{ex_j} / k_{atk}^2}$ 
9:    $Ex' \leftarrow Ex' \setminus \{ex_j\}$ 
10: end while
11: if  $\sum_{D \in Pr_D} Pr_D(D) p(A, D) \leq k_{atk}$  then
12:   return  $A$ 
13: else if  $\sum_{D \in Pr_D} Pr_D(D) p(A \setminus \{ex_j\}, D) \geq$   

    $\sum_{D \in Pr_D} Pr_D(D) p(\{ex_j\}, D)$  then
14:   return  $A \setminus \{ex_j\}$ 
15: else
16:   return  $\{ex_j\}$ 
17: end if
```

[0047] Algorithm for DHDP. When using the overlap payoff function, DHDP can be modeled as a weighted set cover problem. Because the overlap payoff function is a modular function, the associated cost of a given vulnerability v , is simply the payoff produced by the singleton set $\{v\}$ with a mixed attack strategy. In the common case where each constraint set is a singleton set, if the overlap payoff function is used, an adaptation on the standard greedy weighted set cover algorithm can be used for DHDP (Algorithm 3), providing a $\ln(n) + 1$ approximation,

Evaluation and Discussion

[0048] Darknet Market Data. Eight marketplaces located on the Tor network were scraped and parsed during the month of May 2015. Each of these markets host vendors offering “hacking tools”, including malware, botnets, exploits and other means serving to breach, steal and otherwise manipulate virtual targets. The product list is comprised of 235 such hacking tools, 167 of which were distinct.

Algorithm 3 Weighted Greedy DHDP Algorithm for Singleton Constraint Set and Overlap Payoff Function Case

Input: Vulnerabilities V , Pr_A , and application constraints $\mathcal{C}$.

Output: $D \subseteq V$ s.t. the application constraints $\mathcal{C}$ are satisfied.

```
1:  $D \leftarrow \emptyset$ 
2:  $S \leftarrow \text{set s.t. } S_i = \{j : V_j \in \mathcal{C}_i \text{ where } V_j \text{ is } i\text{th vulnerability in } V\}$ 
3:  $c_{S_i} \leftarrow \sum_{A \in Pr_A} Pr_A(A) |Exp(A) \cap \{V_i\}|$ 
4:  $\mathcal{C}' \leftarrow [\mathcal{C}]$ 
5: while  $\mathcal{C}' \neq \emptyset$  do
6:    $S_i \leftarrow \text{argmax}_{g \in S} \frac{|S_i \cap \mathcal{C}'|}{c_{S_i}}$ 
7:    $\mathcal{C}' \leftarrow \mathcal{C}' \setminus S_i$ 
8:    $D \leftarrow D \cup \{V_i\}$ 
9: end while
10: return  $D$ 
```

[0049] It found several identical products being sold on more than one market usually by the same seller (using an identical online handle). The products targeted 21 specific platforms, such as different versions of Adobe Flash, Linux, MSWindows and OS X as well as online presences such as Facebook, Wordpress and others. Hardware-related software such as those associated with Point-of-Sale machines, routers, and servers are also reflected in this number. FIG. 2 illustrates the variety of products in the markets and Table 2 illustrates exemplar exploits.

[0050] System Configurations. As noted in FIG. 2, a variety of platforms were represented in our darknet market data. Results are described using application constraints based on common configurations for Windows and Linux servers - as these were the most prominent targets of exploits found on the darknet. In our experiments, software was mapped such as media players, databases, and FTP server software to application constraint sets to model the functional requirements of a system. Experiments were conducted with models for Android, Point-of-Sale, and Apple systems - though qualitatively the results differed little from the Windows and Linux Server experiments.

[0051] DHAP Results. Both the greedy and multiplicative update approaches were implemented to address the DHAP problem. For the greedy algorithm, three variants of greedy (cost-benefit, uniform cost, and combination of the the two) were studied while we varied the parameter ϵ for the multiplicative update approach. Attacker payoff was examined as a function of budget (in Bitcoin). FIGS. 3A and 3B display this result. Though the cost-benefit greedy algorithm has

the potential to perform poorly, it was, in general, the best performing approach - despite the multiplicative update approach achieving the better approximation guarantee. Further, the multiplicative update algorithm (Algorithm 2) was consistently the slowest in terms of runtime, taking much longer than the lazy greedy algorithms, particularly for high values of k_{atk} . Despite the multiplicative update algorithm having a better theoretical approximation ratio when compared to the tandem of greedy algorithms, namely $(1 - \epsilon) (1 - 1/e)$ compared to $\frac{1}{2}(1 - 1/e)$, as shown in FIGS. **3A** and **3B** that the greedy algorithms performed as good as or better than the multiplicative update very consistently. In all algorithms, as expected, runtime grew with budget (not pictured) - though the relationship was not strict, as an increase in budget does not necessarily mean that more exploits will be selected. In the experiments (on a commodity computer equipped with a 3.49 GHz i7 CPU and 16 GB of memory), the runtimes never exceeded ten minutes.

[0052] DHDP Results. FIGS. **4A** and **4B** demonstrate a defender's best response to an attack strategy against a Windows Server and Linux Server, respectively, for varying values of k_{atk} . Though similar trends are shown in FIGS. **3A** and **3B** as are shown in FIGS. **4A** and **4B**, the payoff is generally lower, meaning that the defender can lower the expected payoff by enacting a best response strategy to an attack strategy produced by DHAP - which in the framework translates to fewer exploited vulnerabilities.

[0053] Exploit Payoff Analysis. Instead of altering the software that appears on the host system in an attempt to avoid exploits, such as in the best response approach, in exploit payoff analysis, the defender will identify which specific exploits are increasing the payoff the most, with a hope that the defender can reverse-engineer the exploit, or patch the vulnerability himself. To identify which exploits should be reverse-engineered, the defender first runs DHAP against his host system to identify what payoff an attacker could expect to produce. Then, for each exploit ex , the defender runs DHAP against the host with the set of exploits $Ex \setminus \{ex\}$. The exploit ex that, when removed from the universe of exploits Ex , produces the largest drop in payoff for the attacker is the exploit that the defender should attempt to reverse-engineer. More formally, let A be the attack strategy produced by DHAP when using Ex as the universe of exploits and let A_{ex} be the attack strategy that is produced when DHAP is run against the host when using $Ex \setminus \{ex\}$ as the universe of exploits. The defender will attempt to reverse-engineer the exploit, where D is the

defense strategy representing the host. To account for exploits that, though they greatly reduce payoff when removed from Ex , may be too expensive for the defender to purchase, a cost-benefit analysis is also considered where the decrease in payoff is normalized by the cost of the exploit. The top exploits to reverse-engineer to defend a Windows Server host when considering an attacker budget of $k_{atk} = 5$, are shown in Table 3 with columns for both maximum payoff reduction and maximum cost-benefit analysis.

Prod.	Vulu.	Target	USD
Kernel Panic	X-display system	Linux <= 3.13.0-43	\$471.56
IE <= 11	memory corr.	IE on Windows <= 7	\$35.00
RemoteShell	wordpress.php	Wordpress MU	\$1,500.00
Delay RCE	WebView memory corr.	Android 4.1, 4.2	\$36.50
WindowsLPE	win32k elev. of priv.	Windows <= 8.1	\$12.00-48.17
MS15-034 RCE	hwp.sys	Windows <= 8.1	\$311.97
PDF Flash Exp.	unpaper	FlashPlayer <= 16.0.0.287	\$600.00

Table 2: Examples of Exploits from Darknet Markets

Exploit	Max. Payoff Reduction	Max. Cost-Benefit	Exploit Cost (BTC)
SMTP Mail Cracker	1	4.757	0.2102
SUPER-S493	1	1.100	0.8404
Hack ICO	1	79.089	0.01264
Plasma	0.6677	1.582	0.2563
Wordpress Exploiter	0.6677	2.6467	0.2102
CVE-2014-0160	0.6677	3.178	0.3161

Table 3: Defender Exploit Analysis for $k_{atk} = 5$

Game Theoretic Framework

In some embodiments, to leverage the data collected from the darknet, a game theoretic framework is disclosed to reason about a defender facing an attacker sourced through the communities on the darknet. The paradigm used for this is based on the framework of a “security game”. Such a framework 500 is designed from the ground-up to consider marketplace information a simplified block diagram is shown in FIG. 5. In this framework, an attacker has a strategy (denoted A) that consists of a set of exploits he must purchase within a given budget. An exploit function (denoted Ex) maps the attacker’s strategy to a set of vulnerable software applications, which can be easily obtained from darknet marketplace data.

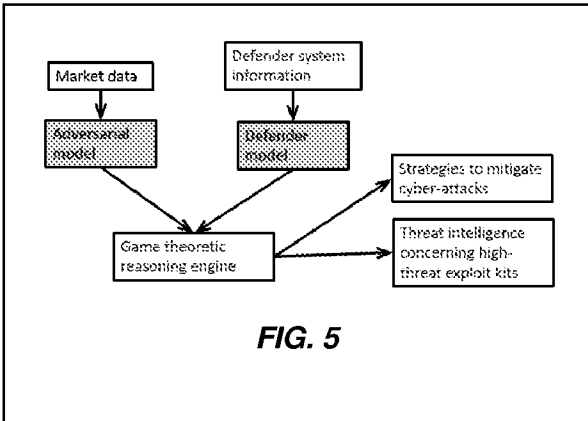


FIG. 5

Meanwhile, the set of applications on a defender's system D is treated as his strategy. While the payoff function is defined in terms of axioms, a simple payoff function can be the cardinality of the overlap -- $p(A,D) = |Ex(A) \cap D|$. The NP-hard problems of finding optimal strategies for both players and developed approximation algorithms are disclosed. A mixed strategy of attack and defense is disclosed that provides a natural extension for populations of computer systems as opposed to a single host as well as the modeling of multiple attackers.

[0054] Referring to FIG. 6, a detailed description of an example computing system 600 having one or more computing units that may implement various systems and methods discussed herein is provided. The computing system 600 may be applicable to the system described herein. For example, the computing system 600 may form a portion of the theoretical game engine 504 of FIG. 5 discussed above. It will be appreciated that specific implementations of these devices may be of differing possible specific computing architectures not all of which are specifically discussed herein but will be understood by those of ordinary skill in the art.

[0055] The computer system 600 may be a computing system is capable of executing a computer program product to execute a computer process. Data and program files may be input to the computer system 600, which reads the files and executes the programs therein. Some of the elements of the computer system 600 are shown in FIG. 6, including one or more hardware processors 602, one or more data storage devices 604, one or more memory devices 606, and/or one or more ports 608-612. Additionally, other elements that will be recognized by those skilled in the art may be included in the computing system 600 but are not explicitly depicted in Fig. 6 or discussed further herein. Various elements of the computer system 600 may communicate with one another by way of one or more communication buses, point-to-point communication paths, or other communication means not explicitly depicted in FIG. 6.

[0056] The processor 602 may include, for example, a central processing unit (CPU), a microprocessor, a microcontroller, a digital signal processor (DSP), and/or one or more internal levels of cache. There may be one or more processors 602, such that the processor comprises a single central-processing unit, or a plurality of processing units capable of executing instructions and performing

operations in parallel with each other, commonly referred to as a parallel processing environment.

[0057] The computer system 600 may be a conventional computer, a distributed computer, or any other type of computer, such as one or more external computers made available via a cloud computing architecture. The presently described technology is optionally implemented in software stored on the data stored device(s) 604, stored on the memory device(s) 606, and/or communicated via one or more of the ports 608-612, thereby transforming the computer system 600 in FIG. 6 to a special purpose machine for implementing the operations described herein. Examples of the computer system 600 include personal computers, terminals, workstations, mobile phones, tablets, laptops, personal computers, multimedia consoles, gaming consoles, set top boxes, and the like.

[0058] The one or more data storage devices 604 may include any non-volatile data storage device capable of storing data generated or employed within the computing system 600, such as computer executable instructions for performing a computer process, which may include instructions of both application programs and an operating system (OS) that manages the various components of the computing system 600. The data storage devices 604 may include, without limitation, magnetic disk drives, optical disk drives, solid state drives (SSDs), flash drives, and the like. The data storage devices 604 may include removable data storage media, non-removable data storage media, and/or external storage devices made available via a wired or wireless network architecture with such computer program products, including one or more database management products, web server products, application server products, and/or other additional software components. Examples of removable data storage media include Compact Disc Read-Only Memory (CD-ROM), Digital Versatile Disc Read-Only Memory (DVD-ROM), magneto-optical disks, flash drives, and the like. Examples of non-removable data storage media include internal magnetic hard disks, SSDs, and the like. The one or more memory devices 606 may include volatile memory (e.g., dynamic random access memory (DRAM), static random access memory (SRAM), etc.) and/or non-volatile memory (e.g., read-only memory (ROM), flash memory, etc.).

[0059] Computer program products containing mechanisms to effectuate the systems and methods in accordance with the presently described technology may reside in the data storage devices 604 and/or the memory devices

606, which may be referred to as machine-readable media. It will be appreciated that machine-readable media may include any tangible non-transitory medium that is capable of storing or encoding instructions to perform any one or more of the operations of the present disclosure for execution by a machine or that is capable of storing or encoding data structures and/or modules utilized by or associated with such instructions. Machine-readable media may include a single medium or multiple media (e.g., a centralized or distributed database, and/or associated caches and servers) that store the one or more executable instructions or data structures.

[0060] In some implementations, the computer system 600 includes one or more ports, such as an input/output (I/O) port 608, a communication port 610, and a sub-systems port 612, for communicating with other computing, network, or vehicle devices. It will be appreciated that the ports 608-612 may be combined or separate and that more or fewer ports may be included in the computer system 600.

[0061] The I/O port 608 may be connected to an I/O device, or other device, by which information is input to or output from the computing system 600. Such I/O devices may include, without limitation, one or more input devices, output devices, and/or environment transducer devices.

[0062] In one implementation, the input devices convert a human-generated signal, such as, human voice, physical movement, physical touch or pressure, and/or the like, into electrical signals as input data into the computing system 600 via the I/O port 608. Similarly, the output devices may convert electrical signals received from computing system 600 via the I/O port 608 into signals that may be sensed as output by a human, such as sound, light, and/or touch. The input device may be an alphanumeric input device, including alphanumeric and other keys for communicating information and/or command selections to the processor 602 via the I/O port 608. The input device may be another type of user input device including, but not limited to: direction and selection control devices, such as a mouse, a trackball, cursor direction keys, a joystick, and/or a wheel; one or more sensors, such as a camera, a microphone, a positional sensor, an orientation sensor, a gravitational sensor, an inertial sensor, and/or an accelerometer; and/or a touch-sensitive display screen ("touchscreen"). The output devices may include, without limitation, a display, a touchscreen, a speaker, a tactile and/or haptic output device, and/or the like. In some implementations, the input device and the output device may be the same device, for example, in the case of a touchscreen.

[0063] In one implementation, a communication port 610 is connected to a network by way of which the computer system 600 may receive network data useful in executing the methods and systems set out herein as well as transmitting information and network configuration changes determined thereby. Stated differently, the communication port 610 connects the computer system 600 to one or more communication interface devices configured to transmit and/or receive information between the computing system 600 and other devices by way of one or more wired or wireless communication networks or connections. For example, the computer system 600 may be instructed to access information stored in a public network, such as the Internet. The computer 600 may then utilize the communication port to access one or more publicly available servers that store information in the public network. In one particular embodiment, the computer system 600 uses an Internet browser program to access a publicly available website. The website is hosted on one or more storage servers accessible through the public network. Once accessed, data stored on the one or more storage servers may be obtained or retrieved and stored in the memory device(s) 606 of the computer system 600 for use by the various modules and units of the system, as described herein.

[0064] Examples of types of networks or connections of the computer system 600 include, without limitation, Universal Serial Bus (USB), Ethernet, Wi-Fi, Bluetooth®, Near Field Communication (NFC), Long-Term Evolution (LTE), and so on. One or more such communication interface devices may be utilized via the communication port 610 to communicate one or more other machines, either directly over a point-to-point communication path, over a wide area network (WAN) (e.g., the Internet), over a local area network (LAN), over a cellular (e.g., third generation (3G) or fourth generation (4G)) network, or over another communication means. Further, the communication port 610 may communicate with an antenna for electromagnetic signal transmission and/or reception.

[0065] The computer system 600 may include a sub-systems port 612 for communicating with one or more additional systems to perform the operations described herein. For example, the computer system 600 may communicate through the sub-systems port 612 with a large processing system to perform one or more of the calculations discussed above.

[0066] The system set forth in FIG. 6 is but one possible example of a computer system that may employ or be configured in accordance with aspects of the present disclosure. It will be appreciated that other non-transitory tangible computer-readable storage media storing computer-executable instructions for implementing the presently disclosed technology on a computing system may be utilized.

[0067] FIG. 7 is a flowchart of a method for applying game theoretic cyber threat mitigation to a network. In one particular embodiment, the operations of the method 700 may be executed by the computing device described above in relation to FIG. 6. Thus, the computing device may utilize a network connection to a public network to obtain a set of exploits to attack a device or network, such as in operation 702. In some instances, the set of exploits may be obtained from the darknet portion of the Internet. In operation 704, the computing device creates a constraint set of vulnerabilities of a network under attack. In general, the constraint set of vulnerabilities includes those vulnerabilities in the attacked device or network that are required for some system functionality. In operation 706, the computing device applies the set of exploits to the constraint set of vulnerabilities of the attacked network to determine a success on attacking the network. In operation 708, the computing device may reverse engineer one or more of the set of exploits applied to the attacked network to develop a patch to the exposed vulnerability to the network.

[0068] It should be understood from the foregoing that, while particular embodiments have been illustrated and described, various modifications can be made thereto without departing from the spirit and scope of the invention as will be apparent to those skilled in the art. Such changes and modifications are within the scope and teachings of this invention as defined in the claims appended hereto.

CLAIMS

What is claimed is:

1. A system for protecting a computer system from attack, the system comprising:
 - a network connection for communicating with a public network;
 - a processing device; and
 - a computer-readable medium connected to the processing device configured to store instructions that, when executed by the processing device, performs the operations of:
 - obtaining a set of exploits from the public network through the network connection, the set of exploits configured to penetrate the computer system;
 - creating a constraint set of vulnerabilities of the computer system comprising a minimum set of dependencies to operate the computer system;
 - applying the set of exploits to the computer system;
 - analyzing the application of the set of exploits on the computer system to detect a particular vulnerability of the computer system; and
 - altering a configuration of the computer system in response to the analysis of the application of the set of exploits.
2. The system of claim 1, wherein analyzing the application of the set of exploits on the computer system comprises quantifying a risk level posed to the computer system related to a cost to obtain the set of exploits.
3. The system of claim 2, wherein the public network is the Internet and the processing device further performs the operation of:
 - aligning Internet data with the constraint set of vulnerabilities based on information obtained about the set of exploits.

4. The system of claim 3, wherein obtaining a set of exploits from the public network through the network connection comprises:
 - applying one or more algorithms to obtain the set of exploits based on the constraint set of vulnerabilities of the computer system from one or more darknet marketplaces on the Internet.
5. The system of claim 4, wherein the one or more algorithms determine the cost to obtain the set of exploits to create a budget and obtains the set of exploits constrained by the determined cost to obtain the set of exploits.
6. The system of claim 5, wherein obtaining the set of exploits is based on maximizing the quantifying of the risk level posed to the computer system related to the cost to obtain the set of exploits
7. The system of claim 1, wherein altering the configuration of the computer system comprises removing a software component of the computer system that is utilized by the set of exploits to attack the computer system.
8. A method for improving a computing device, the method comprising:
 - obtaining a set of exploits from a public network, the set of exploits configured to bypass a security feature of the computer system;
 - analyzing an application of the set of exploits on the computer system to detect a particular vulnerability of the computer system; and
 - altering a configuration of the computer system in response to the analysis of the application of the set of exploits.
9. The method of claim 8 further comprising:
 - creating a constraint set of vulnerabilities of the computer system comprising a minimum set of dependencies to operate the computer system; and

wherein the application of the set of exploits on the computer system comprises determining the effect of the set of exploits on the constraint set of vulnerabilities of the computer system.

10. The method of claim 9, wherein analyzing the application of the set of exploits on the computer system comprises quantifying a risk level posed to the computer system related to a cost to obtain the set of exploits from the public network.
11. The method of claim 10, further comprising:
 - aligning public network data with the constraint set of vulnerabilities based on information obtained about the set of exploits.
12. The method of claim 11, wherein obtaining a set of exploits from the public network comprises:
 - applying one or more algorithms to obtain the set of exploits based on the constraint set of vulnerabilities of the computer system from one or more darknet marketplaces on the Internet.
13. The method of claim 12, wherein the one or more algorithms determine the cost to obtain the set of exploits to create a budget and obtains the set of exploits constrained by the determined cost to obtain the set of exploits.
14. The method of claim 13, wherein obtaining the set of exploits is based on maximizing the quantifying of the risk level posed to the computer system related to the cost to obtain the set of exploits.
15. The method of claim 8, wherein altering the configuration of the computer system comprises removing a software component of the computer system that is utilized by the set of exploits to attack the computer system.

16. The method of claim 8, wherein altering the configuration of the computer system comprises installing a patch to a software component of the computer system that is exposed by the set of exploits to attack the computer system.
17. One or more non-transitory tangible computer-readable storage media storing computer-executable instructions for performing a computer process on a machine, the computer process comprising:
 - obtaining a set of exploits from a public network, the set of exploits configured to bypass a security feature of the computer system;
 - analyzing an application of the set of exploits on the computer system to detect a particular vulnerability of the computer system; and
 - altering a configuration of the computer system in response to the analysis of the application of the set of exploits.
18. The one or more non-transitory computer-readable storage media of claim 17, wherein the computer process further comprises:
 - creating a constraint set of vulnerabilities of the computer system comprising a minimum set of dependencies to operate the computer system; and
 - wherein the application of the set of exploits on the computer system comprises determining the effect of the set of exploits on the constraint set of vulnerabilities of the computer system.
19. The one or more non-transitory computer-readable storage media of claim 17, wherein analyzing the application of the set of exploits on the computer system comprises quantifying a risk level posed to the computer system related to a cost to obtain the set of exploits from the public network.
20. The one or more non-transitory computer-readable storage media of claim 17, wherein obtaining a set of exploits from the public network comprises applying one or more algorithms to obtain the set of exploits from one or more darknet marketplaces on the Internet.

ABSTRACT

System and methods for a data-driven security game framework that models an attacker based on exploit market data actively mined from the darknet to develop strategies for the defender are disclosed.

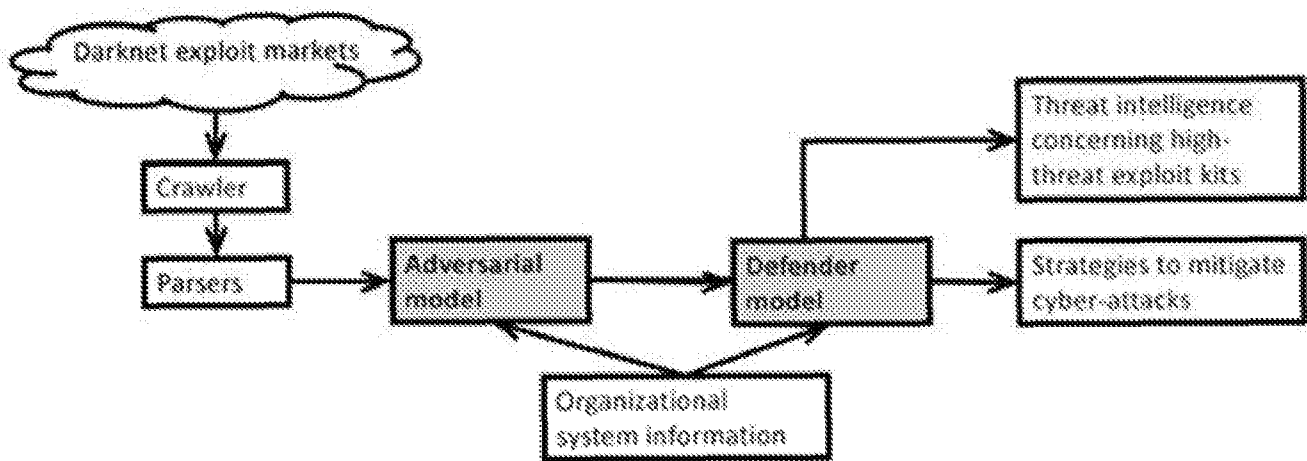


Fig. 1

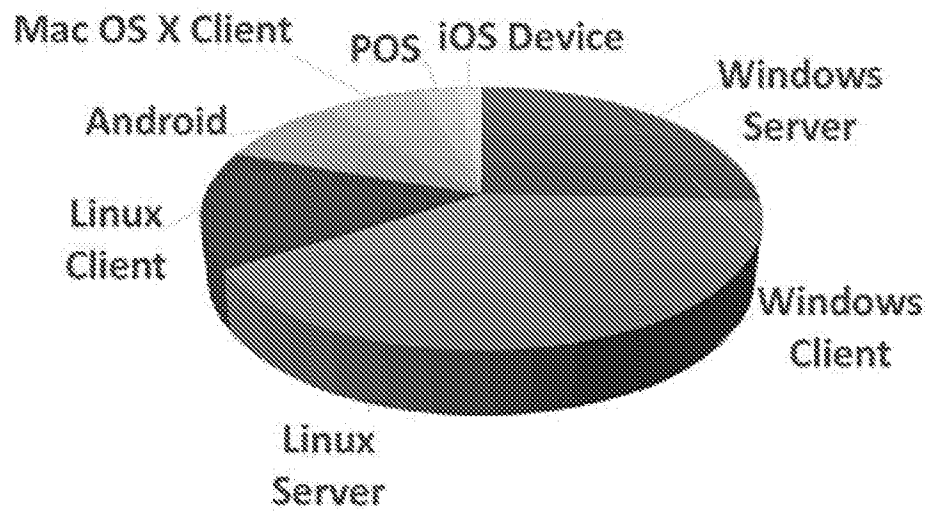


Fig. 2

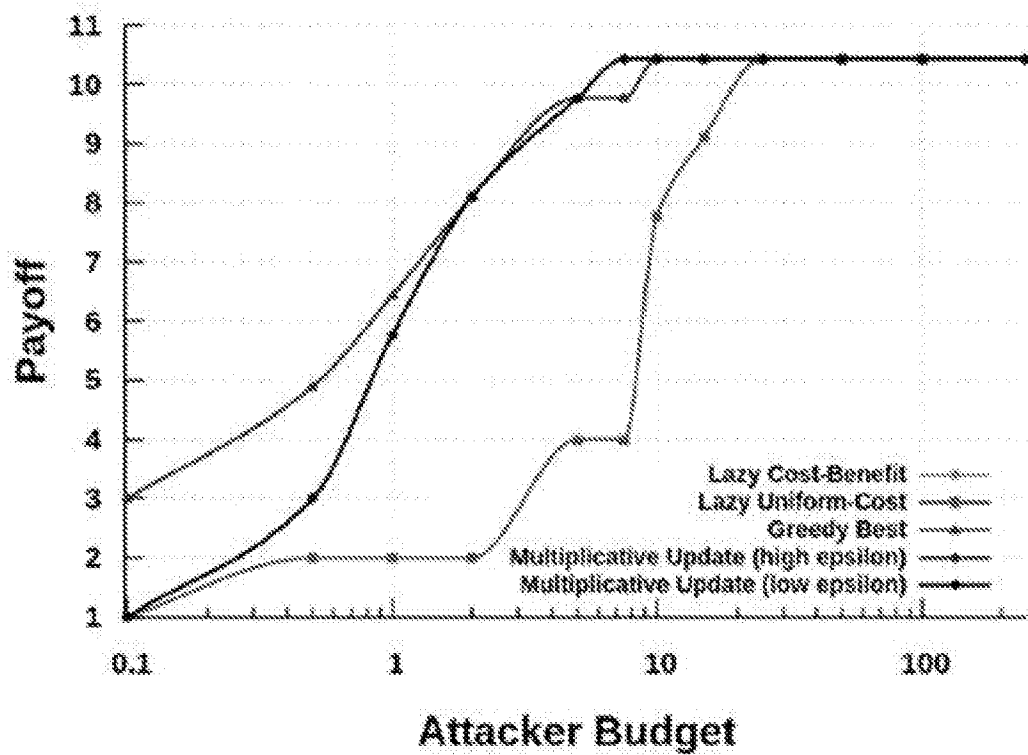


Fig. 3A

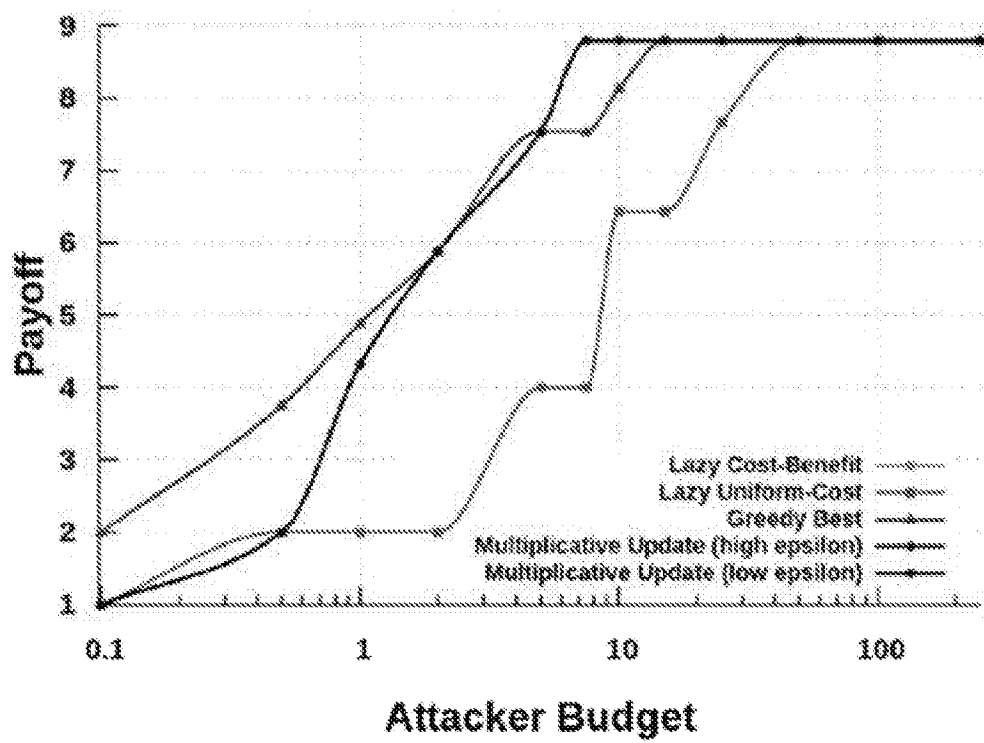


Fig. 3B

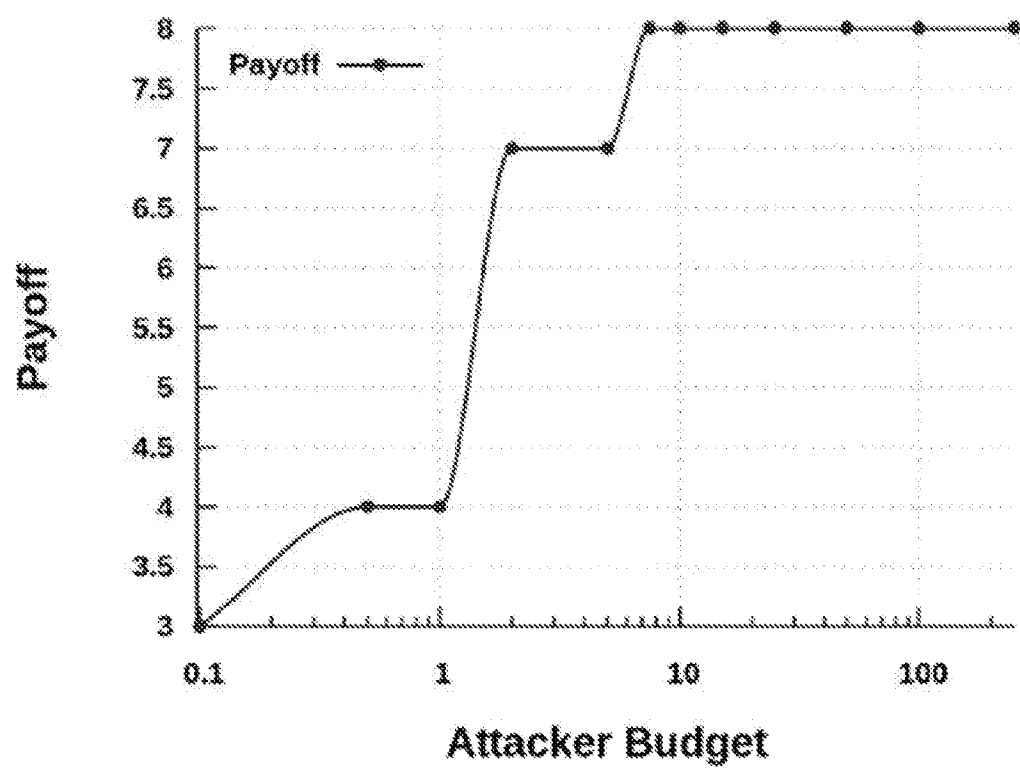


Fig. 4A

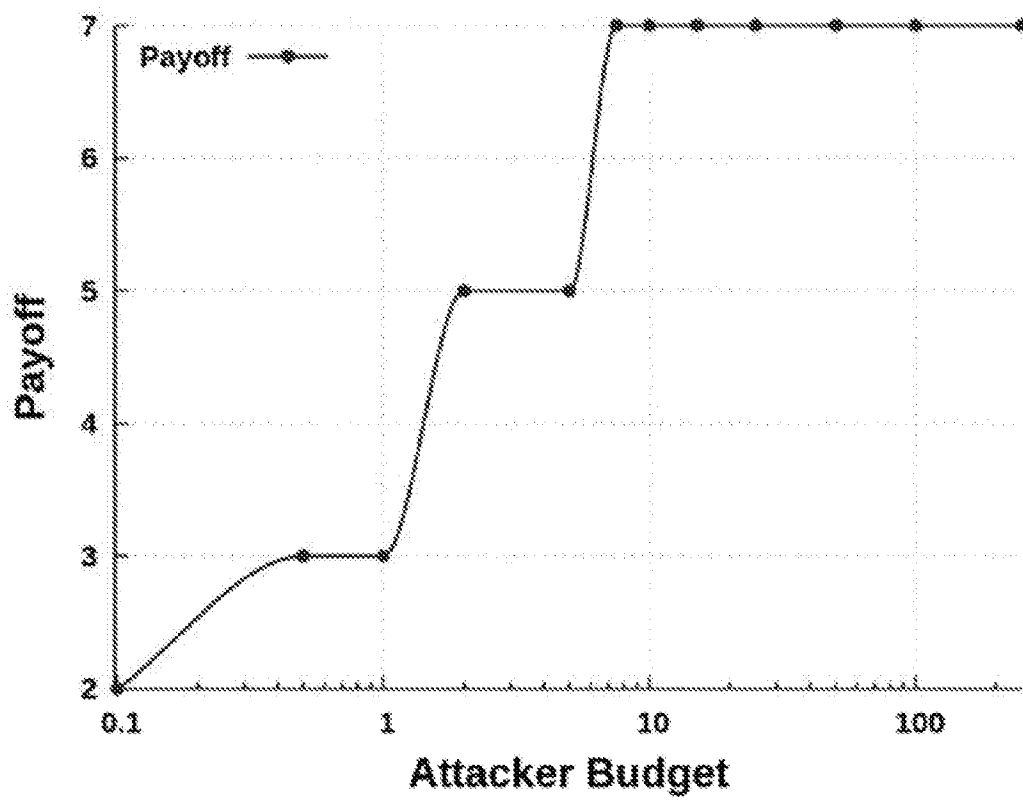


Fig. 4B

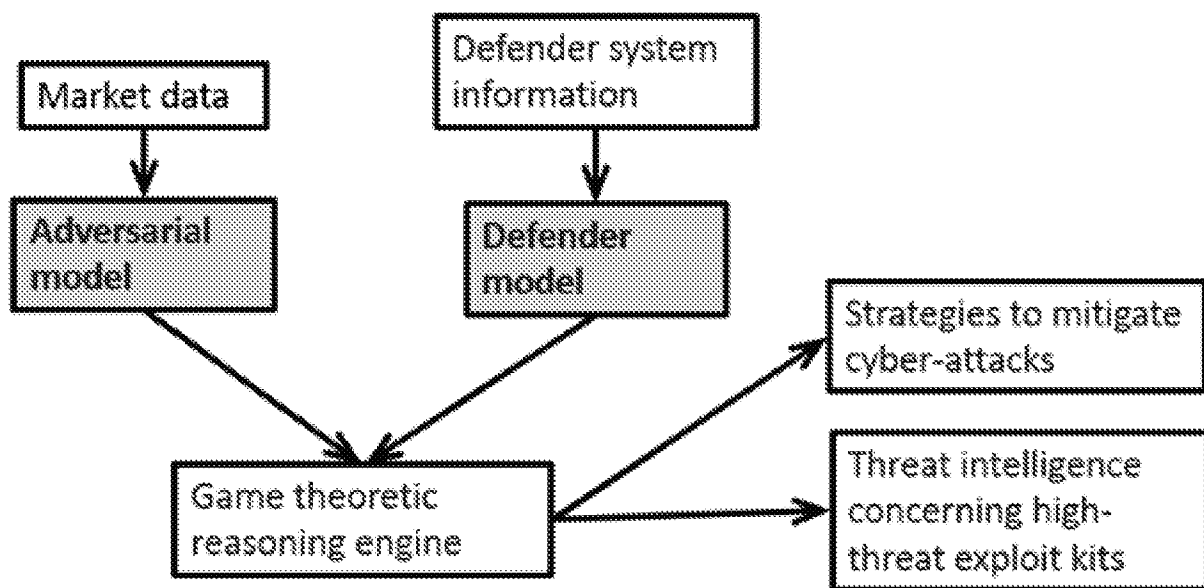


Fig. 5

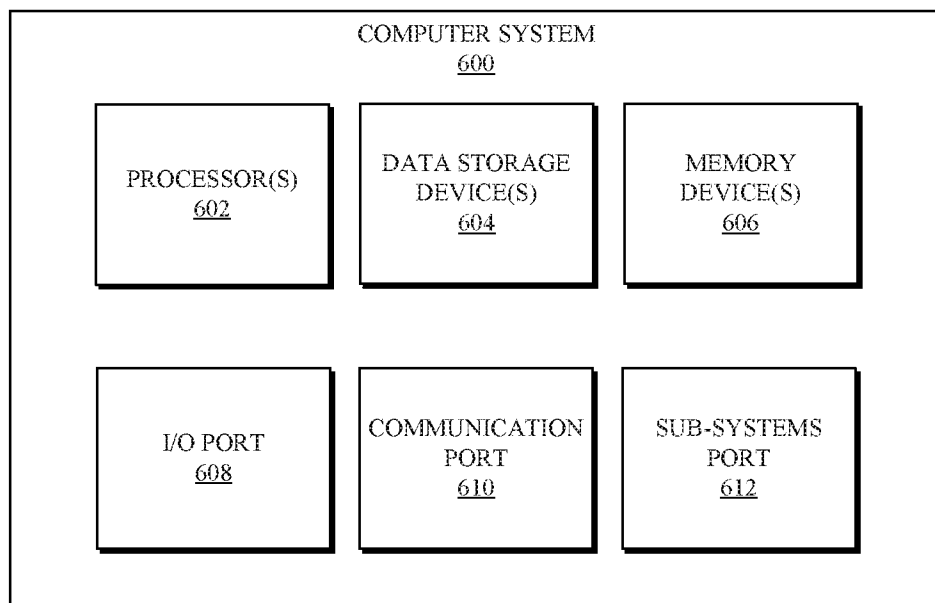


FIG. 6

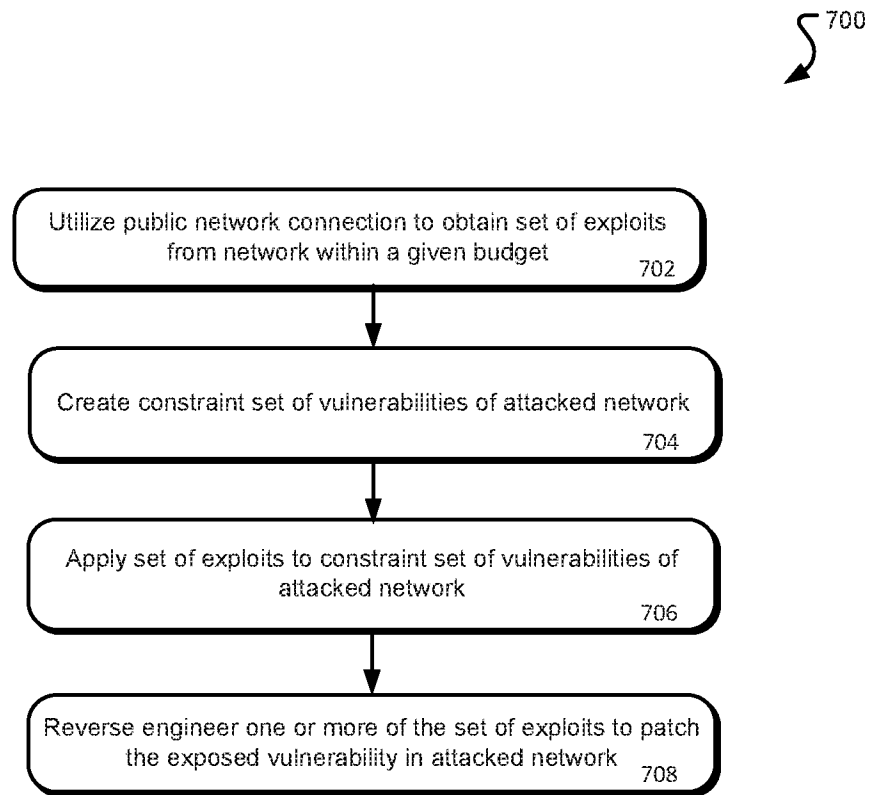


FIG. 7

SCORE Placeholder Sheet for IFW Content

Application Number: 15362730

Document Date: 11/28/2016

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 below.

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://Score.uspto.gov/ScoreAccessWeb/>).
- External customers may access SCORE content via the Public and Private PAIR interfaces.



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
15/362,730	11/28/2016	2431	435	055743-555439	20	3

CONFIRMATION NO. 5936

FILING RECEIPT



0000000087733281

27148
POL SINELLI PC
900 WEST 48TH PLACE
SUITE 900
KANSAS CITY, MO 64112-1895

Date Mailed: 12/09/2016

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**

Inventor(s)

Paulo Shakarian, Chandler, AZ;
John Robertson, Prescott, AZ;
Jana Shakarian, Chandler, AZ;
Vivin Paliath, Chandler, AZ;
Amanda Thart, Scottsdale, AZ;

Applicant(s)

ARIZONA BOARD OF REGENTS ON BEHALF OF ARIZONA STATE UNIVERSITY, Tempe, AZ

Power of Attorney: None

Domestic Priority data as claimed by applicant

This appln claims benefit of 62/261,200 11/30/2015

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 12/07/2016

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/362,730**

Projected Publication Date: 06/01/2017

Non-Publication Request: No

Early Publication Request: No

**** MICRO ENTITY ****

Title

SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT
MITIGATION

Preliminary Class

726

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

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 (1-866-999-4258).

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 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 Assets Control, 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 U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 15/362,730			
APPLICATION AS FILED - PART I									
(Column 1)		(Column 2)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY			
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)		
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	70		
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	150		
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	180		
TOTAL CLAIMS (37 CFR 1.16(j))	20	minus 20 = *			OR	x 20 =	0.00		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3	minus 3 = *				x 105 =	0.00		
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			TOTAL	400		
APPLICATION AS AMENDED - PART II									
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY	
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	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))					OR			
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					OR			
			TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE			
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY	
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	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))					OR			
	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.									



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
15/362,730	11/28/2016	Paulo Shakarian	055743-555439

CONFIRMATION NO. 5936

INFORMAL NOTICE



27148
POL SINELLI PC
900 WEST 48TH PLACE
SUITE 900
KANSAS CITY, MO 64112-1895

Date Mailed: 12/09/2016

INFORMATIONAL NOTICE TO APPLICANT

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

The item(s) indicated below are also required and should be submitted with any reply to this notice to avoid further processing delays.

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):

Paulo Shakarian
John Robertson
Jana Shakarian
Vivin Paliath
Amanda Thart

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/mhaile/

Under the Paperwork Reduction Act of 1996, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)**

Title of Invention	SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION
-------------------------------	---

As the below named inventor, I hereby declare that:

This declaration
is directed to:☐

The attached application, or

☒United States application or PCT international application number 15/362,730filed on November 28, 2016

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001
by fine or imprisonment of not more than five (5) years, or both.**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.

LEGAL NAME OF INVENTORInventor: Amanda ThartDate (Optional): 11/29/16Signature: Amanda Thart

Note: An application data sheet (PTO/AIA/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

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 1 minute 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 22315-1450. 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 this 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 displays a valid OMB control number.

**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)****Title of
Invention****SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER
THREAT MITIGATION**

As the below named inventor, I hereby declare that:

This declaration is directed to: ☐ The attached application, or☒ United States application or PCT international application number 15/362,730
filed on November 28, 2016.

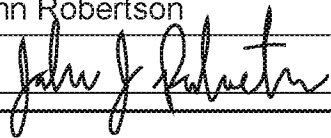
The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

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.

LEGAL NAME OF INVENTORInventor: John Robertson Date (Optional) : _____Signature: 

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

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 1 minute 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.

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.

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.

**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)****Title of
Invention****SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER
THREAT MITIGATION**

As the below named inventor, I hereby declare that:

This declaration
is directed to:☐

The attached application, or

☒United States application or PCT international application number 15/362,730filed on November 28, 2016.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than **five (5)** years, or both.**WARNING:**

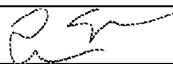
Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization 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.

LEGAL NAME OF INVENTOR

Inventor: Paulo Shakarian

Date (Optional) : _____

Signature: _____



Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

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 1 minute 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.

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.

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.

**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)****Title of
Invention****SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER
THREAT MITIGATION**

As the below named inventor, I hereby declare that:

This declaration
is directed to:☐

The attached application, or

☒United States application or PCT international application number 15/362,730filed on November 28, 2016

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001
by fine or imprisonment of not more than five (5) years, or both.**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.

LEGAL NAME OF INVENTORInventor: Vivin Paliath

Date (Optional): _____

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

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 1 minute 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-8198 and select option 2.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention **SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION**

As the below named inventor, I hereby declare that:

This declaration is directed to: ☐ The attached application, or
☒ United States application or PCT international application number 15/362,730
filed on November 28, 2016

The above-identified application was made or authorized to be made by me.

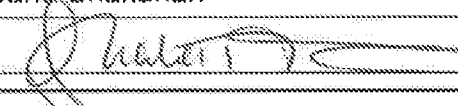
I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

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.

LEGAL NAME OF INVENTOR

Inventor: Jana Shakarian Date (Optional): 11/29/16
Signature: 

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

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 1 minute 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 Acknowledgement Receipt

EFS ID:	27870110
Application Number:	15362730
International Application Number:	
Confirmation Number:	5936
Title of Invention:	SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION
First Named Inventor/Applicant Name:	Paulo Shakarian
Customer Number:	27148
Filer:	Ari M. Bai/Janelle Wiggins
Filer Authorized By:	Ari M. Bai
Attorney Docket Number:	055743-555439
Receipt Date:	21-DEC-2016
Filing Date:	28-NOV-2016
Time Stamp:	17:37:17
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Oath or Declaration filed	055743-555439-Executed-Declaration-Thart.pdf	922356	no	1
			adda6be7b9d61e962be34ac9aa6a03c54e9803df		

Warnings:

IPR2025-01397

Information:					
2	Oath or Declaration filed	055743-555439-Executed-Declaration-Robertson.pdf	96886	no	2
			aed26f8ae71d4c7a348af7d1bf14406ff22ab372		
Warnings:					
Information:					
3	Oath or Declaration filed	055743-555439-Executed-Declaration-Paulo-Shakarian.pdf	134737	no	2
			9c42a41df5acaeb3604977164e07c16f456c4076		
Warnings:					
Information:					
4	Oath or Declaration filed	055743-555439-Executed-Declaration-Paliath.pdf	94565	no	1
			6415991f85345f050278c01fbbbe18db859264e3		
Warnings:					
Information:					
5	Oath or Declaration filed	055743-555439-Executed-Declaration-Jana-Shakarian.pdf	188684	no	1
			7242a1ce4b9d6d9d76de4b928845dcd214189973		
Warnings:					
Information:					
Total Files Size (in bytes):			1437228		
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.					

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA/82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	15/362,730
Filing Date	November 28, 2016
First Named Inventor	Paulo Shakarian, et al.
Title	SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION
Art Unit	2431
Examiner Name	ZECHER, CORDELIA P K
Attorney Docket Number	055743-555439

SIGNATURE of Applicant or Patent Practitioner

Signature	/Ari M. Bai/	Date (Optional)	
Name	Ari M. Bai	Registration Number	38726
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.



*Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.131, 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.

IPR2025-01397

CrowdStrike EX1002 Page 66

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number

Filing Date

15/362,730

November 28, 2016

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)



I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above:

27148

OR



I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:



The address associated with the above-mentioned Customer Number

OR



The address associated with Customer Number:

OR

Firm or
Individual Name

Address

City

State

Zip

Country

Telephone

Email

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

ARIZONA BOARD OF REGENTS ON BEHALF OF ARIZONA STATE UNIVERSITY



Inventor or Joint Inventor (title not required below)



Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)



Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)



Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature

Tamara Deuser

Date (Optional)

4/17/14

Name

Tamara Deuser

Title

Associate Vice President for Operations at OKED, Arizona Board of Regents on Behalf of Arizona State University

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.



Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.131, 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.

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(c)Applicant/Patent Owner: Arizona Board of Regents on Behalf of Arizona State UniversityApplication No./Patent No.: 15/362,730Filed/Issue Date: November 28, 2016Titled: SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATIONArizona Board of Regents on Behalf of Arizona State University, a university

(Name of Assignee)

(Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☒ The assignee of the entire right, title, and interest.
2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):
- ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.
- ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (e.g., bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

- A. ☒ 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 041165, Frame 0676, or for which a copy thereof is attached.
- 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.

[Page 1 of 2]

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.

IPR2025-01397

CrowdStrike EX1002 Page 68

STATEMENT UNDER 37 CFR 3.73(c)

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.

4. 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.

5. 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.

6. 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).

☐ As required by 37 CFR 3.73(c)(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.

/Ari M. Bai/

Signature

Ari M. Bai

Printed or Typed Name

February 15, 2017

Date

Reg. No. 38726

Title or Registration Number

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.

Electronic Acknowledgement Receipt

EFS ID:	28365512
Application Number:	15362730
International Application Number:	
Confirmation Number:	5936
Title of Invention:	SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION
First Named Inventor/Applicant Name:	Paulo Shakarian
Customer Number:	27148
Filer:	Ari M. Bai/Janelle Wiggins
Filer Authorized By:	Ari M. Bai
Attorney Docket Number:	055743-555439
Receipt Date:	15-FEB-2017
Filing Date:	28-NOV-2016
Time Stamp:	15:15:23
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	055743-555439-Executed-POA.pdf	848544 053841553cf4276bcb38a46b60a37aaa6bd7e414	no	2

Warnings:

IPR2025-01397

Information:					
2	Assignee showing of ownership per 37 CFR 3.73	055743-555439-Executed-373c-Statement.pdf	71718	no	3
			60230cbbb648a2bfcfb301b59a9d1b7c30b866e		
Warnings:					
Information:					
Total Files Size (in bytes):			920262		
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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/362,730	11/28/2016	Paulo Shakarian	055743-555439

CONFIRMATION NO. 5936

POA ACCEPTANCE LETTER



27148
POL SINELLI PC
900 WEST 48TH PLACE
SUITE 900
KANSAS CITY, MO 64112-1895

Date Mailed: 02/17/2017

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/15/2017.

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.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/yterferra/



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
15/362,730	11/28/2016	Paulo Shakarian	055743-555439

CONFIRMATION NO. 5936

PUBLICATION NOTICE



OC00000091775641

27148
POL SINELLI PC
900 WEST 48TH PLACE
SUITE 900
KANSAS CITY, MO 64112-1895

Title:SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION

Publication No.US-2017-0155677-A1

Publication Date:06/01/2017

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 (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, 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 Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	15362730
	Filing Date	2016-11-28
	First Named Inventor	Paulo Shakarian
	Art Unit	2495
	Examiner Name	Henry Tsang
	Attorney Docket Number	055743-555439

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	8413238		2013-04-02	Michael Sutton	All	
	2	8863293		2014-10-14	Mihai Christodorescu et al.	All	
	3						

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	20150215332		2015-07-30	Dejan Curcic	All	

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
	1							

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	15362730
Filing Date	2016-11-28
First Named Inventor	Paulo Shakarian
Art Unit	2495
Examiner Name	Henry Tsang
Attorney Docket Number	055743-555439

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

NON-PATENT LITERATURE DOCUMENTS

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	ASHOT ABRAHAMIAN, Application of Stackelberg Security Games in Information Security, 9th Annual Symposium on Information Assurance (Asia '14), June 3-4, 2014, Albany, NY, pp. 62-65	
	2	LILLIAN ABLON, MARTIN C. LIBICKI, ANDREA A. GOLAY, Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar, 2014, National Security Research Division, RAND Corporation.	
	3	YOSSI AZAR, IFTAH GAMZU, Efficient Submodular Function Maximization Under Linear Packing Constraints, in Automata, Languages, and Programming, 39th International Colloquium, ICALP 2012, pp. 38-50, Springer.	
	4	HSINCHUN CHEN, Dark Web: Exploring and Data Mining the Dark Side of the Web, Vol. 30, 2012, Springer Science and Business Media.	
	5	URIEL FEIGE, A Threshold of $\ln n$ for Approximating Set Cover, Journal of the ACM, July 1998, Vol. 45, No. 4, pp. 634-652.	
	6	CHRISTOPHER KIEKINTVELD, VILIAM LISY, RADEK PÍBIL, Game-theoretic Foundations for the Strategic Use of Honeypots in Network Security, in Cyber Warfare - Building the Scientific Foundation, 2015, Vol. 56, pp. 81-101, Springer.	
	7	WEIFENG LI, HSINCHUN CHEN, Identifying Top Sellers in Underground Economy Using Deep Learning-Based Sentiment Analysis, Joint Intelligence and Security Informatics Conference, 2014, pp. 64-67, Institute of Electrical and Electronics Engineers Inc.	
	8	G.L. NEMHAUSER, L.A. WOLSEY, An Analysis of Approximations for Maximizing Submodular Set Functions – I, Mathematical Programming, 1978, Vol. 14, pp. 265-294, North-Holland Publishing Company.	
	9	KIEN C. NGUYEN, TANSU ALPCAN, AND TAMER BASAR, Stochastic Games for Security in Networks with Interdependent Nodes, International Conference on Game Theory for Networks, 2009, pp. 697-703, IEEE.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	15362730
Filing Date	2016-11-28
First Named Inventor	Paulo Shakarian
Art Unit	2495
Examiner Name	Henry Tsang
Attorney Docket Number	055743-555439

10	KYLE SOSKA, NICOLAS CHRISTIN, Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem, in the Proceedings of the 24th USENIX Security Symposium, August 14-15 2015, pp. 33-48, USENIX Association.
11	ZIMING ZHAO, GAIL-JOON AHN, HONGXIN HU, DEEPINDER MAHI, Social Impact: Systematic Analysis of Underground Social Dynamics, in Computer Security – ESORICS 2012, 2012, Sara Foresti, Moti Yung, Fabio Martinelli, eds., pp. 877-894, Springer.
12	KONG-WEI LYE, JEANETTE M WING, Strategies in Network Security, International Journal of Information Security, 2005, Vol. 4, No. 1, pp. 71-86, Springer-Verlag 2005.
13	JURE LESKOVEC, ANDREA KRAUSE, CARLOS GUESTRIN, CHRISTOS FALOUTSOS, JEANNA VANBRIESEN, NATALIE GLANCE, Cost-Effective Outbreak Detection in Networks, In Proceedings of the 13th ACM SIGKDD International conference on Knowledge discovery and data mining, 2007, pp. 420-29, ACM.
14	JOHN ROBERTSON, VIVIN PALIATH, JANA SHAKARIAN, AMANDA THART, PAULO SHAKARIAN, Data Driven Game Theoretic Cyber Threat Mitigation, in Proceedings of the Twenty-Eighth AAAI Conference on Innovative Application (IAAI6), 2016, pp. 4041-4046, Association for the Advancement of Artificial Intelligence.
15	P. SHAKARIAN, Stuxnet: Cyberwar Revolution in Military Affairs, Small Wars Journal, 2011, Small Wars Foundation.
16	SHAKARIAN, LEI, LINDELAUF, Power Grid Defense Against Malicious Cascading Failure, in Proceedings of the 13th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2014), 2014, pp. 813-820, International Foundation for Autonomous Agents and Multiagent Systems.
17	DEVON CALLAHAN, PAULO SHAKARIAN, JEFFREY NIELSON, ANTHONY N. JOHNSON, Shaping Operations to Attack Robust Terror Networks, Socialinformatics, 2014.
18	PAULO SHAKARIAN, AUSTIN PARKER, GERARDO SIMARI, and VENKATRAMANA (V. S.) SUBRAHMANIAN, Annotated Probabilistic Temporal Logic. ACM Transactions on Computational Logic, 2011, Vol. 12, No. 2, Art. 14.

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

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.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	15362730
Filing Date	2016-11-28
First Named Inventor	Paulo Shakarian
Art Unit	2495
Examiner Name	Henry Tsang
Attorney Docket Number	055743-555439

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	15362730
Filing Date	2016-11-28
First Named Inventor	Paulo Shakarian
Art Unit	2495
Examiner Name	Henry Tsang
Attorney Docket Number	055743-555439

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	/Ari M. Bai/	Date (YYYY-MM-DD)	2018-02-01
Name/Print	Ari M. Bai	Registration Number	38726

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.**

Electronic Acknowledgement Receipt

EFS ID:	31679331
Application Number:	15362730
International Application Number:	
Confirmation Number:	5936
Title of Invention:	SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION
First Named Inventor/Applicant Name:	Paulo Shakarian
Customer Number:	27148
Filer:	Ari M. Bai/Helen Miswell
Filer Authorized By:	Ari M. Bai
Attorney Docket Number:	055743-555439
Receipt Date:	01-FEB-2018
Filing Date:	28-NOV-2016
Time Stamp:	18:27:27
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

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)	M16-040P_IDS.pdf	1020182	no	5
			46e46300bb2eb50e4c36e993fdb07ba346868e3		

Warnings:

IPR2025-01397

Information:					
A U.S. Patent Number Citation is required in the Information Disclosure Statement (IDS) form. You may remove the form to add the required data in order to correct the Informational Message or if you chose not to, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
2	Non Patent Literature	2_AblonMarketsForCybercrime 2014.pdf	2132856 3da67df68cf310cf62ae7ec7e02e9613f050789c	no	85
Warnings:					
Information:					
3	Non Patent Literature	4_ChenDarkWeb2012.pdf	10731537 dd35ec58912488366b2adfd6bbaafaea3be25458	no	478
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
4	Non Patent Literature	5_FeigeAThresholdofInn1998. pdf	155752 83dc5ee478bfdca626b8bc413b98a7e024d5698c	no	19
Warnings:					
Information:					
5	Non Patent Literature	6_KeikintveldGame- Theoretic2015.pdf	721095 c42dad937e99a589bb2ff4c847088cf1c3843d03	no	21
Warnings:					
Information:					
6	Non Patent Literature	7_LilidentifyingTopSellers2014. pdf	182341 260616727bc42a4a4da9d3156b40d39280f4ae02	no	4
Warnings:					
Information:					
7	Non Patent Literature	8_NemhauserApproximationsF orMaximizing1978.pdf	1243305 b9e43395663f74c581982e9ca97a0d7057a0008c	no	30
Warnings:					
Information:					

8	Non Patent Literature	9_NguyenStochasticGamesforSecurity2009.pdf	331767	no	7
			3c5497fe35d48a2b40e9c0eb3a16e492374f8d4f		
Warnings:					
Information:					
9	Non Patent Literature	10_SoskaMeasuringTheLongitudinal2015.pdf	1243694	no	17
			01f2e7f3dee35c2c7b9179d8eb46f4f766c101d1		
Warnings:					
Information:					
10	Non Patent Literature	11_ZhaoSocialImpactnSystemicAnalysis2012.pdf	15299525	no	911
			5fba55668a0344f03d12325f58319c9e968b6e02		
Warnings:					
Information:					
11	Non Patent Literature	12_LyeGameStrategies2005.pdf	877299	no	17
			5d95b7fa5e5c092240c53dceee3fb57542ea35a2		
Warnings:					
Information:					
12	Non Patent Literature	13_LeskovecCost-EffecticeOutbreak2007.pdf	1106204	no	10
			58826abcd82eb4615875261e35e70ccc4b5cd3e7		
Warnings:					
Information:					
13	Non Patent Literature	14_PublishedInventorShakarianDataDriven2016.pdf	775406	no	6
			7ed781d74560003a1c426a5ebe4e7fc08955df39		
Warnings:					
Information:					
14	Non Patent Literature	16_ShakarianPowerGridDefense2014.pdf	1775276	no	8
			7c73cdebff03c55782a1e0dc774260b5f38f9a017		
Warnings:					
Information:					

15	Non Patent Literature	1_ApplicationofStackelbergSecurity.pdf	110495	no	3
			1cf3077b9f3c203a2ab86d6a79a186b6a602e971		
Warnings:					
Information:					
16	Non Patent Literature	3_AzarEfficientSubmodular2012.pdf	10440771	no	889
			3b2e7e182e33a3a316350cd10e39ba94ba80beb2		
Warnings:					
Information:					
17	Non Patent Literature	15_ShakarianStuxnetnCyberwar2011.pdf	272310	no	10
			fd7da23923f2c9472c0cf2093f2b0d3e41bb91c3		
Warnings:					
Information:					
18	Non Patent Literature	17_CallahanShapingOperations2014.pdf	459937	no	10
			22e3a019efc8ce448638ef7513598b091e6195d4		
Warnings:					
Information:					
19	Non Patent Literature	18_ShakarianAnnotatedProbabilistic2011.pdf	777038	no	44
			a20c2704ebd7e4de98273ed0ff11329d6609aec0		
Warnings:					
Information:					
Total Files Size (in bytes):			49656790		

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.



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.
15/362,730	11/28/2016	Paulo Shakarian	055743-555439	5936
27148	7590	10/15/2018	EXAMINER	
POL SINELLI PC			TSANG, HENRY	
900 WEST 48TH PLACE			ART UNIT	
SUITE 900			PAPER NUMBER	
KANSAS CITY, MO 64112-1895			2495	
			NOTIFICATION DATE	
			DELIVERY MODE	
			10/15/2018	
			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):

uspt@polsinelli.com

DETAILED ACTION

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Information Disclosure Statement

The information disclosure statement (IDS) submitted by applicant dated 02/01/2018 has been considered by the examiner.

Drawings

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: 100, 102, 104, 106, 500, 504. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

Claim 1 is objected to because of the following informalities: the claim recites a computer-readable medium. It is suggested to amend the limitation to a non-transitory computer-readable medium.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-20 are rejected under 35 U.S.C. 101 because the claimed invention is directed to a judicial exception (i.e., a law of nature, a natural phenomenon, or an abstract idea) without significantly more. Claims 1-7 are directed to a machine, Claims 8-16 are directed to a process, and Claims 17-20 are directed to a manufacture. Claims 1-20 are directed to an abstract idea (An Idea 'Of Itself') of "collecting and comparing known information", "Comparing information regarding a sample or test subject to a control or target data", "Comparing new and stored information and using rules to identify options", "Diagnosing an abnormal condition by performing clinical tests and thinking about the results" and "Obtaining and comparing intangible data" (e.g. obtaining step, creating step, applying step, analyzing step and altering step, etc). Claims 1-20 are also directed to an abstract idea of "Comparing data to determine a risk level", "Offer-based price optimization", "Budgeting" (e.g. quantifying risk level, determine cost, create budget, etc). Additional elements or combination of elements in the claims other than the abstract idea amount to no more than: mere instructions to implement the abstract idea on generic computer components, and/or recitation of generic computer structure(s). Viewed as a whole and as an ordered combination, the additional claim elements do not provide meaningful limitations to transform the abstract idea such that the claims amount to significantly more than the abstract idea itself. Therefore, Claims 1-20 are rejected under 35 U.S.C. 101 as being directed to non-statutory matter.

Claim Rejections - 35 USC § 103

In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

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

A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 7-9 and 15-18 are rejected under 35 U.S.C. 103 as being unpatentable over Norman et al. US2004/0088565 hereinafter referred to as Norman, in view of Wolff US2013/0198848, and Martinez et al. US2014/0137257 hereinafter referred to as Martinez.

As per claim 1, Norman teaches a system for protecting a computer system from attack, the system comprising: a network connection for communicating with a public network; a processing device; and a computer-readable medium connected to the processing device configured to store instructions that, when executed by the processing device, performs the operations of: obtaining a set of exploits through the network connection, the set of exploits configured to penetrate the computer system (Norman paragraph [0013], [0052], [0055], [0058], [0061], [0067], [0068], obtain and apply exploits);

applying the set of exploits to the computer system (Norman paragraph [0013], [0052], [0055], [0058], [0061], [0067], [0068], apply exploits);

analyzing the application of the set of exploits on the computer system to detect a particular vulnerability of the computer system (Norman paragraph [0013], [0052], [0055], [0058], [0061], [0067], [0068]-[0070], detect vulnerability); and

altering a configuration of the computer system in response to the analysis of the application of the set of exploits (Norman paragraph [0050], [0055], [0059], [0064], [0067], [0069]-[0070], apply remediation).

Norman does not explicitly disclose obtaining a set of exploits from public network through network connection.

Wolff teaches obtaining a set of exploits from public network through network connection (Wolff paragraph [0018]-[0021], [0023]-[0027], obtain exploits).

Thus it would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the invention of Norman with the teachings of Wolff to include obtaining exploits from the public network such as the darknet in order to obtain, analyze and better understand the threats that exists and the vulnerabilities of the system in order to remediate those vulnerabilities.

Norman in view of Wolff does not explicitly disclose creating a constraint set of vulnerabilities of computer system comprising a minimum set of dependencies to operate the computer system.

Martinez teaches creating a constraint set of vulnerabilities of computer system comprising a minimum set of dependencies to operate the computer system (Martinez paragraph [0048], [0083], [0088], [0095], [0109], [0113]-[0114], [0116], [0120], set of vulnerabilities).

Thus it would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the invention of Norman in view of Wolff with the teachings of Martinez to include creating a constraint set of vulnerabilities in order to prioritize the vulnerabilities of the system and to perform security testing and remediation of high risk vulnerabilities.

As per claim 7, Norman in view of Wolff and Martinez teaches the system of claim 1, wherein altering the configuration of the computer system comprises removing a software component of the computer system that is utilized by the set of exploits to attack the computer system (Norman paragraph [0050], [0055], [0059], [0064], [0067], [0069]-[0070]; Wolff paragraph [0028]).

As per claims 8, 15 and 17, claims 8, 15 and 17 claim a method and a non-transitory tangible computer-readable storage media essentially corresponding to the system claims 1 and 7 above, and they are rejected, at least for the same reasons.

As per claim 9, Norman in view of Wolff and Martinez teaches the method of claim 8 further comprising: creating a constraint set of vulnerabilities of the computer system comprising a minimum set of dependencies to operate the computer system; and wherein the application of the set of exploits on the computer system comprises determining the effect of the set of exploits on the constraint set of vulnerabilities of the computer system (Norman paragraph [0013], [0052], [0055], [0058], [0061], [0067], [0068]; Martinez paragraph [0048], [0083], [0088], [0095], [0109], [0113]-[0114], [0116], [0120], [0124]; Wolff paragraph [0018]-[0021], [0023]-[0027]).

As per claim 16, Norman in view of Wolff and Martinez teaches the method of claim 8, wherein altering the configuration of the computer system comprises installing a patch to a software component of

the computer system that is exposed by the set of exploits to attack the computer system (Norman paragraph [0050], [0055], [0059], [0064], [0067], [0069]-[0070]; Wolff paragraph [0028]).

As per claim 18, claim 18 claims a non-transitory tangible computer-readable storage media essentially corresponding to the method claim 9 above, and is rejected, at least for the same reasons.

Claims 2-6, 9-14, 19 and 20 are rejected under 35 U.S.C. 103 as being unpatentable over Norman in view of Wolff and Martinez, and further in view of Frei et al. "International Vulnerability Purchase Program" hereinafter referred to as Frei.

As per claim 2, Norman in view of Wolff and Martinez teaches the system of claim 1, wherein analyzing the application of the set of exploits on the computer system comprises quantifying a risk level posed to the computer system (Norman paragraph [0013], [0052], [0055], [0058], [0061], [0067], [0068]-[0070]; Martinez paragraph [0048], [0083], [0088]-[0090], [0095], [0109], [0113]-[0114], [0116], [0120], [0129]).

Norman in view of Wolff and Martinez does not explicitly disclose quantifying a risk level posed to computer system related to a cost to obtain set of exploits.

Frei teaches quantifying a risk level posed to computer system related to a cost to obtain set of exploits (Frei page 2, 8, 9, 11-13, risk vs. cost of exploits).

Thus it would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the invention of Norman in view of Wolff and Martinez of obtaining exploits from the darknet with the teachings of Frei to include quantifying a cost of the risk of the vulnerabilities to the cost of purchasing the exploit in order to determine to purchase relevant exploits and to purchase the exploits when the cost of the exploits is less than the cost of the risk.

As per claim 3, Norman in view of Wolff, Martinez and Frei teaches the system of claim 2, wherein the public network is the Internet and the processing device further performs the operation of: aligning Internet data with the constraint set of vulnerabilities based on information obtained about the set of exploits (Norman paragraph [0013], [0052], [0055], [0058], [0061], [0067], [0068]; Wolff paragraph

[0018]-[0021], [0023]-[0027], [0044]-[0045]; Martinez paragraph [0048], [0083], [0088], [0095], [0109], [0113]-[0114], [0116], [0120]-[0121]).

As per claim 4, Norman in view of Wolff, Martinez and Frei teaches the system of claim 3, wherein obtaining a set of exploits from the public network through the network connection comprises: applying one or more algorithms to obtain the set of exploits based on the constraint set of vulnerabilities of the computer system from one or more darknet marketplaces on the Internet (Wolff paragraph [0018]-[0021], [0023]-[0027], [0044]-[0045]; Martinez paragraph [0048], [0083], [0088], [0095], [0109], [0113]-[0114], [0116], [0120], [0189], [0207]; Frei page 2, 8, 9, 11-13).

As per claim 5, Norman in view of Wolff, Martinez and Frei teaches the system of claim 4, wherein the one or more algorithms determine the cost to obtain the set of exploits to create a budget and obtains the set of exploits constrained by the determined cost to obtain the set of exploits (Wolff paragraph [0018]-[0021], [0023]-[0027]; Frei page 2, 8, 9, 11-13).

As per claim 6, Norman in view of Wolff, Martinez and Frei teaches the system of claim 5, wherein obtaining the set of exploits is based on maximizing the quantifying of the risk level posed to the computer system related to the cost to obtain the set of exploits (Norman paragraph [0013], [0052], [0055], [0058], [0061], [0067], [0068]-[0070]; Martinez paragraph [0048], [0083], [0088]-[0090], [0095], [0109], [0113]-[0114], [0116], [0120], [0129]; Wolff paragraph [0018]-[0021], [0023]-[0027]; Frei page 2, 8, 9, 11-13).

As per claims 10-14, 19 and 20, claims 10-14, 19 and 20 claim a method and a non-transitory tangible computer-readable storage media essentially corresponding to the system claims 2-6 above, and they are rejected, at least for the same reasons.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HENRY TSANG whose telephone number is (571)270-7959. The examiner can normally be reached on M-F 8am - 5pm EST.

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 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.

/HENRY TSANG/
Primary Examiner, Art Unit 2495

Notice of References Cited	Application/Control No. 15/362,730		Applicant(s)/Patent Under Reexamination Shakarian et al.	
	Examiner HENRY TSANG		Art Unit 2495	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20040088565-A1	05-2004	Norman, Andrew Patrick	H04L63/1433	726/22
*	B	US-20130198848-A1	08-2013	Wolff, Todd	G06F21/568	726/25
*	C	US-20140137257-A1	05-2014	Martinez, Ralph	H04L63/1433	726/25
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Frei et al., "International Vulnerability Purchase Program", NSS Labs, December 2013 (Year: 2013)
	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.

<i>Search Notes</i> 	Application/Control No. 15/362,730	Applicant(s)/Patent Under Reexamination Shakarian et al.
	Examiner HENRY TSANG	Art Unit 2495

CPC - Searched*		
Symbol	Date	Examiner
H04L63/1433 keywords	10/10/2018	HT
H04L63 keywords	10/10/2018	HT

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Inventer/Assignee search in EAST	10/10/2018	HT
EAST text search with keywords	10/10/2018	HT

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
H04L63	keywords	10/10/2018	HT

/HENRY TSANG/ Primary Examiner, Art Unit 2495	
--	--

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S41	3	((("Shakarian") near3 ("Paulo"))).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2018/10/07 14:46
S42	705	((("Robertson") near3 ("John"))).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2018/10/07 14:46
S43	1	((("Shakarian") near3 ("Jana"))).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2018/10/07 14:46
S44	1	((("Paliath") near3 ("Vivin"))).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2018/10/07 14:46
S45	1	((("Thart") near3 ("Amanda"))).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2018/10/07 14:46
S48	1	((("Robertson") near3 ("John"))).INV. and ((exploit\$3 or vulnerab\$7) and cost and budget)	US-PGPUB; USPAT; USOCR	ADJ	ON	2018/10/07 14:59
S49	24	((("Robertson") near3 ("John"))).INV. and (exploit\$3 or vulnerab\$7)	US-PGPUB; USPAT; USOCR	ADJ	ON	2018/10/07 14:59
S50	1958	(ARIZONA near2 BOARD with UNIVERSITY).as. or (ARIZONA near2 BOARD with UNIVERSITY).aanm.	US-PGPUB; USPAT; USOCR	ADJ	ON	2018/10/07 15:00
S51	12	S50 and (exploit\$3 or vulnerab\$7) and cost and budget	US-PGPUB; USPAT; USOCR	ADJ	ON	2018/10/07 15:01
S52	3	S50 and (exploit\$3 or vulnerab\$7) and attack\$3 and defend\$3	US-PGPUB; USPAT; USOCR	ADJ	ON	2018/10/07 15:33
S53	10	S50 and (cost\$3benefit or uniform\$3cost)	US-PGPUB; USPAT; USOCR	ADJ	ON	2018/10/07 15:37
S97	170	((purchas\$3 or cost or price) near4 (exploit or vulnerab\$5 or tool)) and ((penetration or vulnerab\$7 or exploit\$3) near4 test\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2018/10/10 19:05
S98	26	((purchas\$3 or price or cost) near4 (exploit or vulnerab\$5) same budget)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2018/10/10 19:05
S99	50	(cost\$2benefit or uniform\$2cost) and ((purchas\$3 or obtain\$3) with (exploit or vulnerab\$5 or penetration)) and test\$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2018/10/10 19:06
S100	57	((purchas\$3 or cost or price) near4 (exploit or vulnerab\$5 or tool)) and ((penetration or vulnerab\$7 or exploit\$3) near4 test\$3) and h04l63/1433.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2018/10/10 19:08
S101	68	((purchas\$3 or cost or price) near4	US-PGPUB;	ADJ	ON	2018/10/10

IPR2025-01397

		((exploit or vulnerab\$5 or tool)) and ((penetration or vulnerab\$7 or exploit\$3) near4 test\$3) and h04l63\$.cpc.	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			19:08
--	--	---	--	--	--	-------

EAST Search History (I nterference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S102	1	h04l63\$.cpc. and ((exploit or vulnerab\$5) and budget and cost and (darknet or black\$2market)).clm.	US-PGPUB; USPAT	ADJ	ON	2018/10/10 19:11
S103	1	((exploit or vulnerab\$5) and budget and cost and (darknet or black\$2market)).clm.	US-PGPUB; USPAT	ADJ	ON	2018/10/10 19:11
S104	1	((exploit or vulnerab\$5) and risk and cost and (darknet or black\$2market)).clm.	US-PGPUB; USPAT	ADJ	ON	2018/10/10 19:11

10/ 10/ 2018 7:34:24 PM
C:\ Users\ htsang\ Documents\ EAST\ Workspaces\ 15362730.w sp



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. 5936

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.		
15/362,730	11/28/2016	726	2495	055743-555439		
APPLICANTS ARIZONA BOARD OF REGENTS ON BEHALF OF ARIZONA STATE UNIVERSITY, Tempe, AZ INVENTORS Paulo Shakarian, Chandler, AZ; John Robertson, Prescott, AZ; Jana Shakarian, Chandler, AZ; Vivin Paliath, Chandler, AZ; Amanda Thart, Scottsdale, AZ; ** CONTINUING DATA ***** This appln claims benefit of 62/261,200 11/30/2015 ** FOREIGN APPLICATIONS ***** ** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** ** MICRO ENTITY ** 12/07/2016						
Foreign Priority claimed ☐ Yes ☒ No 35 USC 119(a-d) conditions met ☐ Yes ☒ No Verified and Acknowledged <u>/HENRY TSANG/</u> Examiner's Signature		☐ Met after Allowance Initials	STATE OR COUNTRY AZ	SHEETS DRAWINGS 9	TOTAL CLAIMS 20	INDEPENDENT CLAIMS 3
ADDRESS POLSINELLI PC 900 WEST 48TH PLACE SUITE 900 KANSAS CITY, MO 64112-1895 UNITED STATES						
TITLE SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION						
FILING FEE RECEIVED 435	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		

Doc code: IDS

PTO/SB/08a (03-15)

Doc description: Information Disclosure Statement (IDS) Filed

Approved for use through 07/31/2016. 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	15362730
Filing Date	2016-11-28
First Named Inventor	Paulo Shakarian
Art Unit	2495
Examiner Name	Henry Tsang
Attorney Docket Number	055743-555439

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	8413238		2013-04-02	Michael Sutton	All
	2	8863293		2014-10-14	Mihai Christodorescu et al.	All
	3					

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	20150215332		2015-07-30	Dejan Curcic	All

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 ²ⁱ	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
	1							

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15362730
Filing Date	2016-11-28
First Named Inventor	Paulo Shakarian
Art Unit	2495
Examiner Name	Henry Tsang
Attorney Docket Number	055743-555439

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	ASHOT ABRAHAMYAN, Application of Stackelberg Security Games in Information Security, 9th Annual Symposium on Information Assurance (Asia '14), June 3-4, 2014, Albany, NY, pp. 62-65	
	2	LILLIAN ABLON, MARTIN C. LIBICKI, ANDREA A. GOLAY, Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar, 2014, National Security Research Division, RAND Corporation.	
	3	YOSSI AZAR, IFTAH GAMZU, Efficient Submodular Function Maximization Under Linear Packing Constraints, in Automata, Languages, and Programming, 39th International Colloquium, ICALP 2012, pp. 38-50, Springer.	
	4	HSINCHUN CHEN, Dark Web: Exploring and Data Mining the Dark Side of the Web, Vol. 30, 2012, Springer Science and Business Media.	
	5	URIEL FEIGE, A Threshold of $\ln n$ for Approximating Set Cover, Journal of the ACM, July 1998, Vol. 45, No. 4, pp. 634-652.	
	6	CHRISTOPHER KIEKINTVELD, VILIAM LISY, RADEK PÍBIL, Game-theoretic Foundations for the Strategic Use of Honeypots in Network Security, in Cyber Warfare - Building the Scientific Foundation, 2015, Vol. 56, pp. 81-101, Springer.	
	7	WEIFENG LI, HSINCHUN CHEN, Identifying Top Sellers in Underground Economy Using Deep Learning-Based Sentiment Analysis, Joint Intelligence and Security Informatics Conference, 2014, pp. 64-67, Institute of Electrical and Electronics Engineers Inc.	
	8	G.L. NEMHAUSER, L.A. WOLSEY, An Analysis of Approximations for Maximizing Submodular Set Functions – I, Mathematical Programming, 1978, Vol. 14, pp. 265-294, North-Holland Publishing Company.	
	9	KIEN C. NGUYEN, TANSU ALPCAN, AND TAMER BASAR, Stochastic Games for Security in Networks with Interdependent Nodes, International Conference on Game Theory for Networks, 2009, pp. 697-703, IEEE.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number	15362730
Filing Date	2016-11-28
First Named Inventor	Paulo Shakarian
Art Unit	2495
Examiner Name	Henry Tsang
Attorney Docket Number	055743-555439

10	KYLE SOSKA, NICOLAS CHRISTIN, Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem, in the Proceedings of the 24th USENIX Security Symposium, August 14-15 2015, pp. 33-48, USENIX Association.
11	ZIMING ZHAO, GAIL-JOON AHN, HONGXIN HU, DEEPINDER MAHI, Social Impact: Systematic Analysis of Underground Social Dynamics, in Computer Security – ESORICS 2012, 2012, Sara Foresti, Moti Yung, Fabio Martinelli, eds., pp. 877-894, Springer.
12	KONG-WEI LYE, JEANETTE M WING, Strategies in Network Security, International Journal of Information Security, 2005, Vol. 4, No. 1, pp. 71-86, Springer-Verlag 2005.
13	JURE LESKOVEC, ANDREA KRAUSE, CARLOS GUESTRIN, CHRISTOS FALOUTSOS, JEANNA VANBRIESEN, NATALIE GLANCE, Cost-Effective Outbreak Detection in Networks, In Proceedings of the 13th ACM SIGKDD International conference on Knowledge discovery and data mining, 2007, pp. 420-29, ACM.
14	JOHN ROBERTSON, VIVIN PALIATH, JANA SHAKARIAN, AMANDA THART, PAULO SHAKARIAN, Data Driven Game Theoretic Cyber Threat Mitigation, in Proceedings of the Twenty-Eighth AAAI Conference on Innovative Application (IAAI6), 2016, pp. 4041-4046, Association for the Advancement of Artificial Intelligence.
15	P. SHAKARIAN, Stuxnet: Cyberwar Revolution in Military Affairs, Small Wars Journal, 2011, Small Wars Foundation.
16	SHAKARIAN, LEI, LINDELAUF, Power Grid Defense Against Malicious Cascading Failure, in Proceedings of the 13th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2014), 2014, pp. 813-820, International Foundation for Autonomous Agents and Multiagent Systems.
17	DEVON CALLAHAN, PAULO SHAKARIAN, JEFFREY NIELSON, ANTHONY N. JOHNSON, Shaping Operations to Attack Robust Terror Networks, Socialinformatics, 2014.
18	PAULO SHAKARIAN, AUSTIN PARKER, GERARDO SIMARI, and VENKATRAMANA (V. S.) SUBRAHMANYAN, Annotated Probabilistic Temporal Logic. ACM Transactions on Computational Logic, 2011, Vol. 12, No. 2, Art. 14.

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

EXAMINER SIGNATURE

Examiner Signature	/HENRY TSANG/	Date Considered	10/08/2018
--------------------	---------------	-----------------	------------

*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.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		15362730
Filing Date		2016-11-28
First Named Inventor	Paulo Shakarian	
Art Unit		2495
Examiner Name	Henry Tsang	
Attorney Docket Number		055743-555439

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	15362730
Filing Date	2016-11-28
First Named Inventor	Paulo Shakarian
Art Unit	2495
Examiner Name	Henry Tsang
Attorney Docket Number	055743-555439

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	/Ari M. Bai/	Date (YYYY-MM-DD)	2018-02-01
Name/Print	Ari M. Bai	Registration Number	38726

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.**

SCORE Placeholder Sheet for IFW Content

Application Number: 15362730

Document Date: 02/15/2019

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.

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.

- Drawing

At the time of document entry (noted above):

- USPTO employees may access SCORE content via eDAN using the Supplemental Content tab, or via the SCORE web page.
- External customers may access SCORE content via PAIR using the Supplemental Content tab.

100

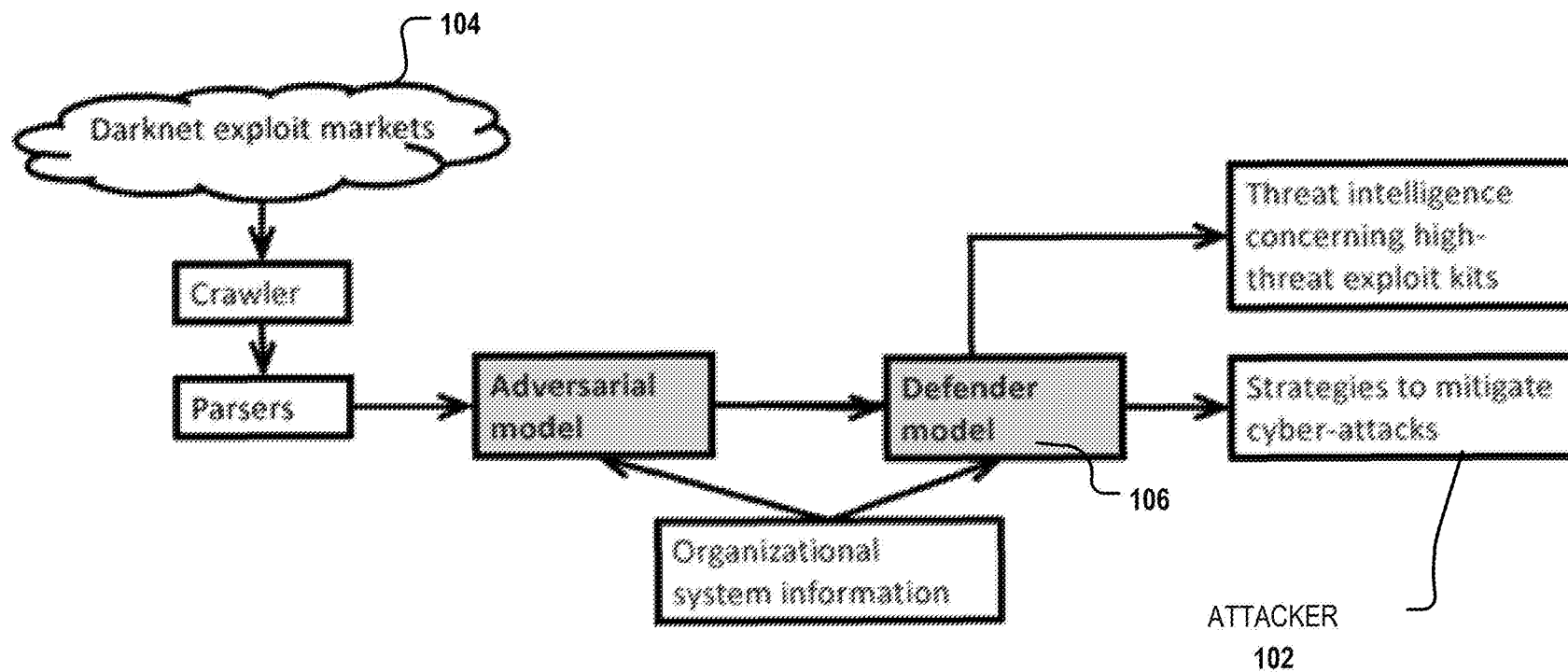


Fig. 1

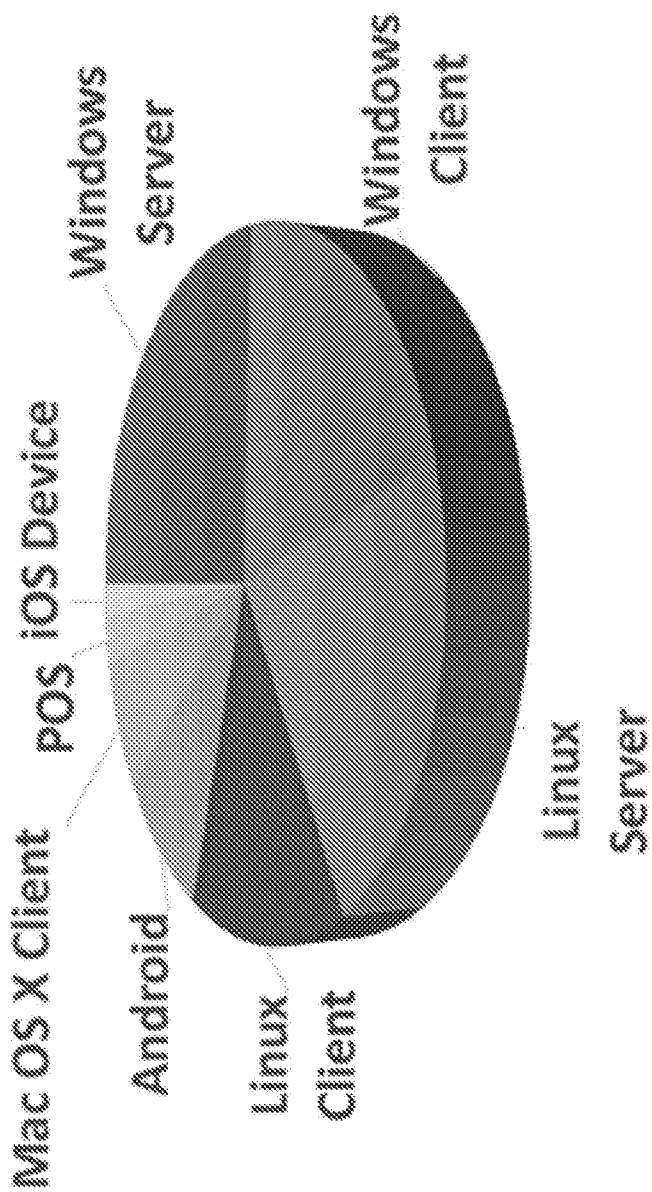


Fig. 2

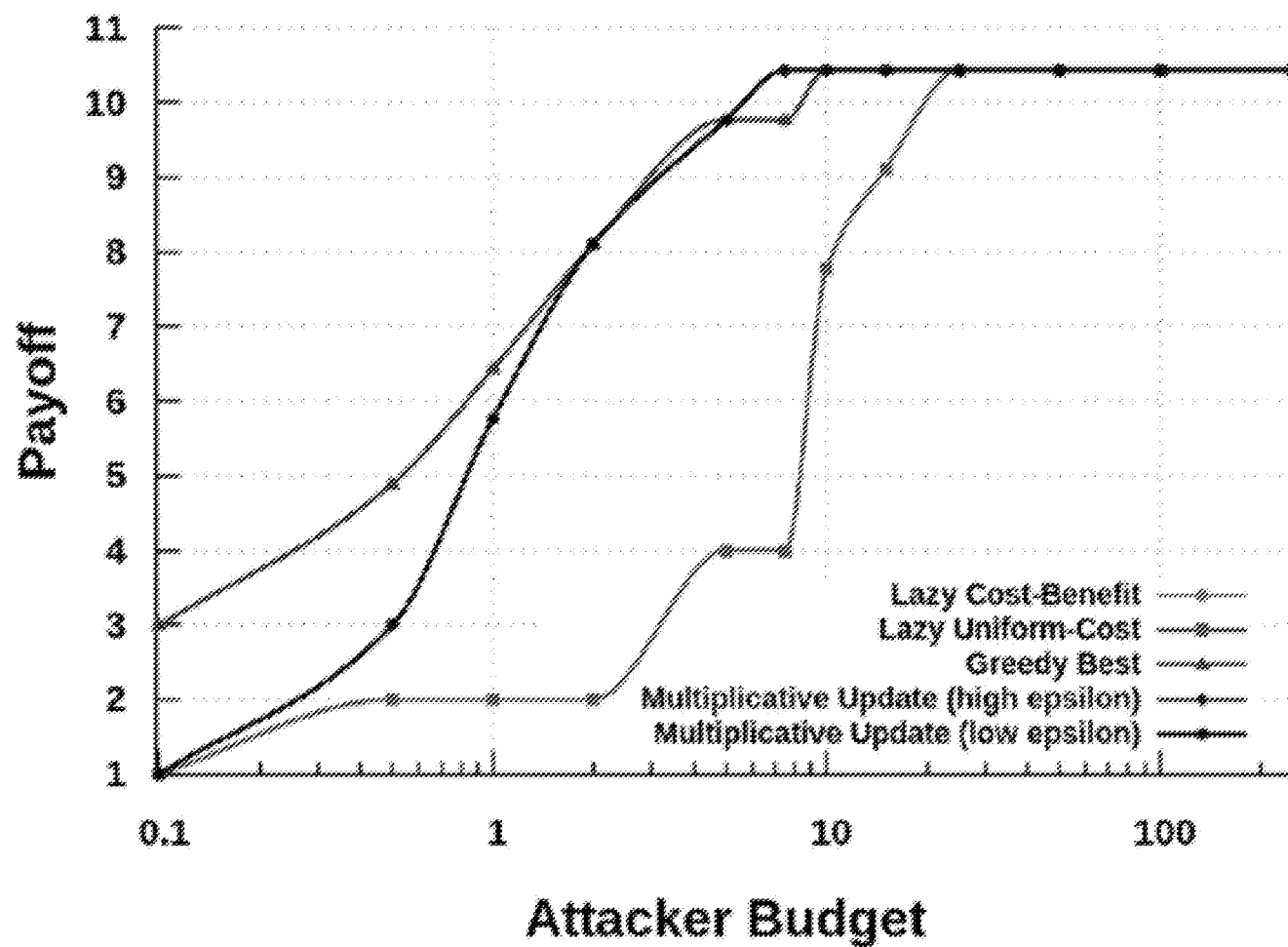


Fig. 3A

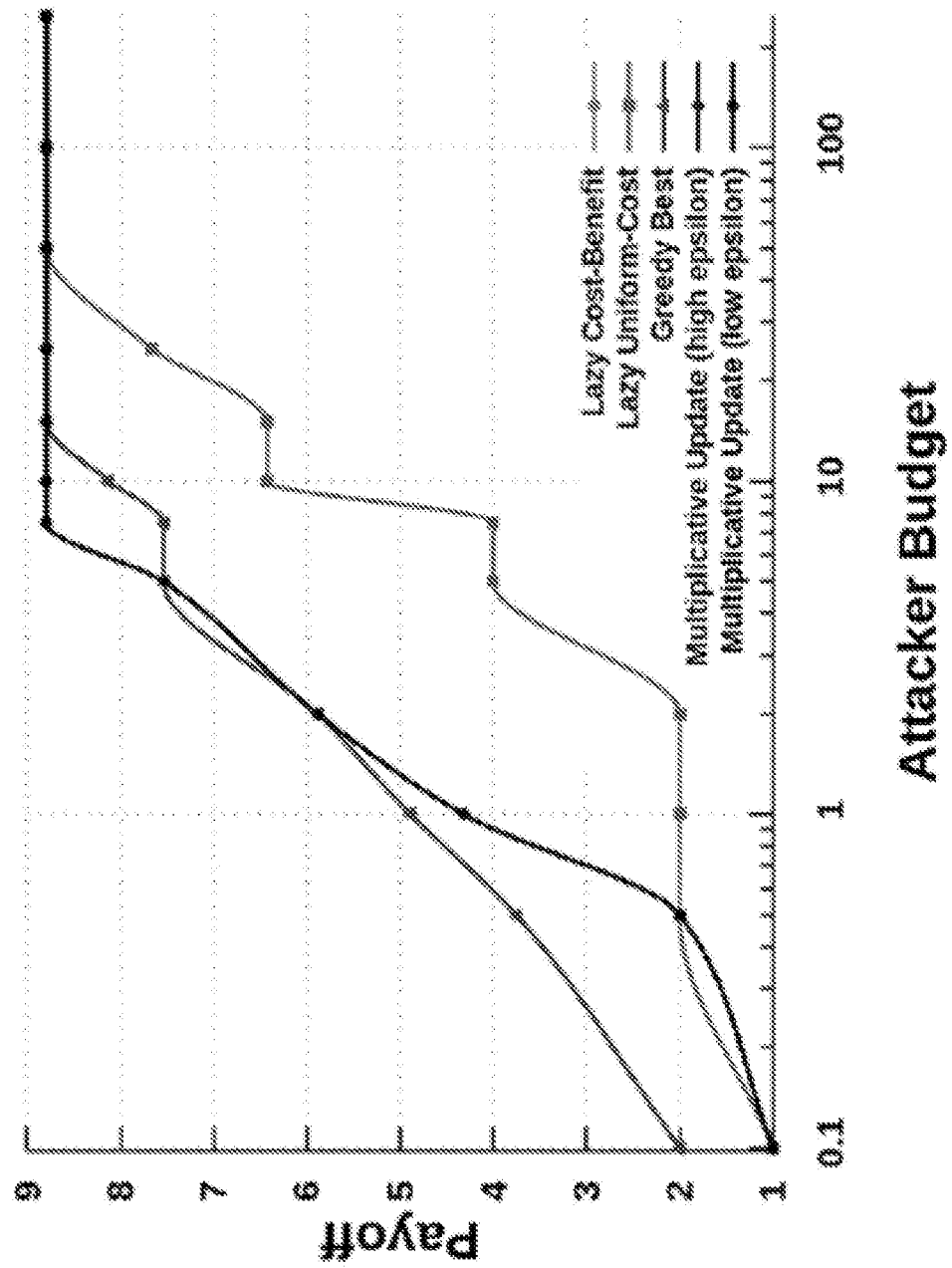


Fig. 3B

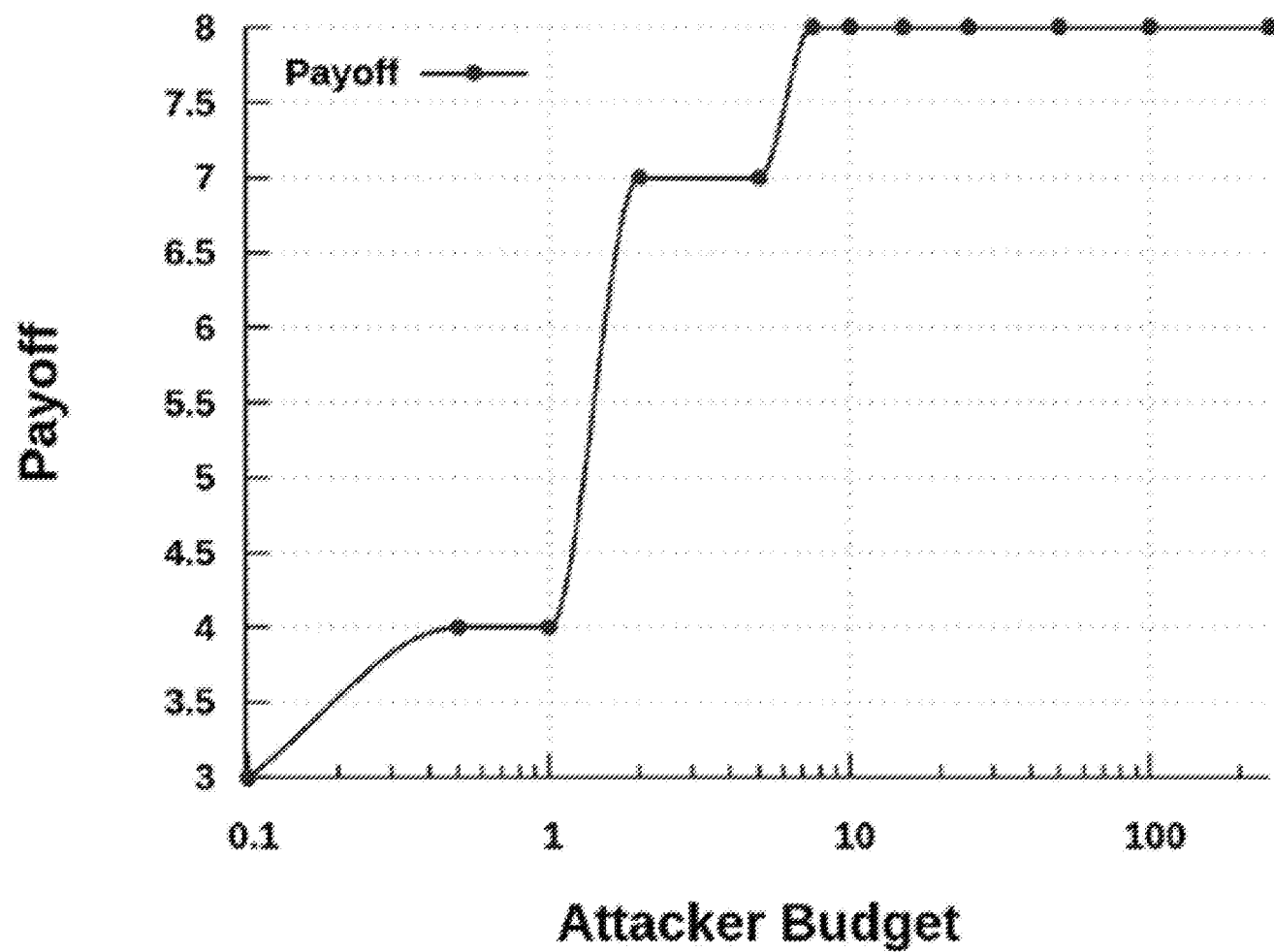


Fig. 4A

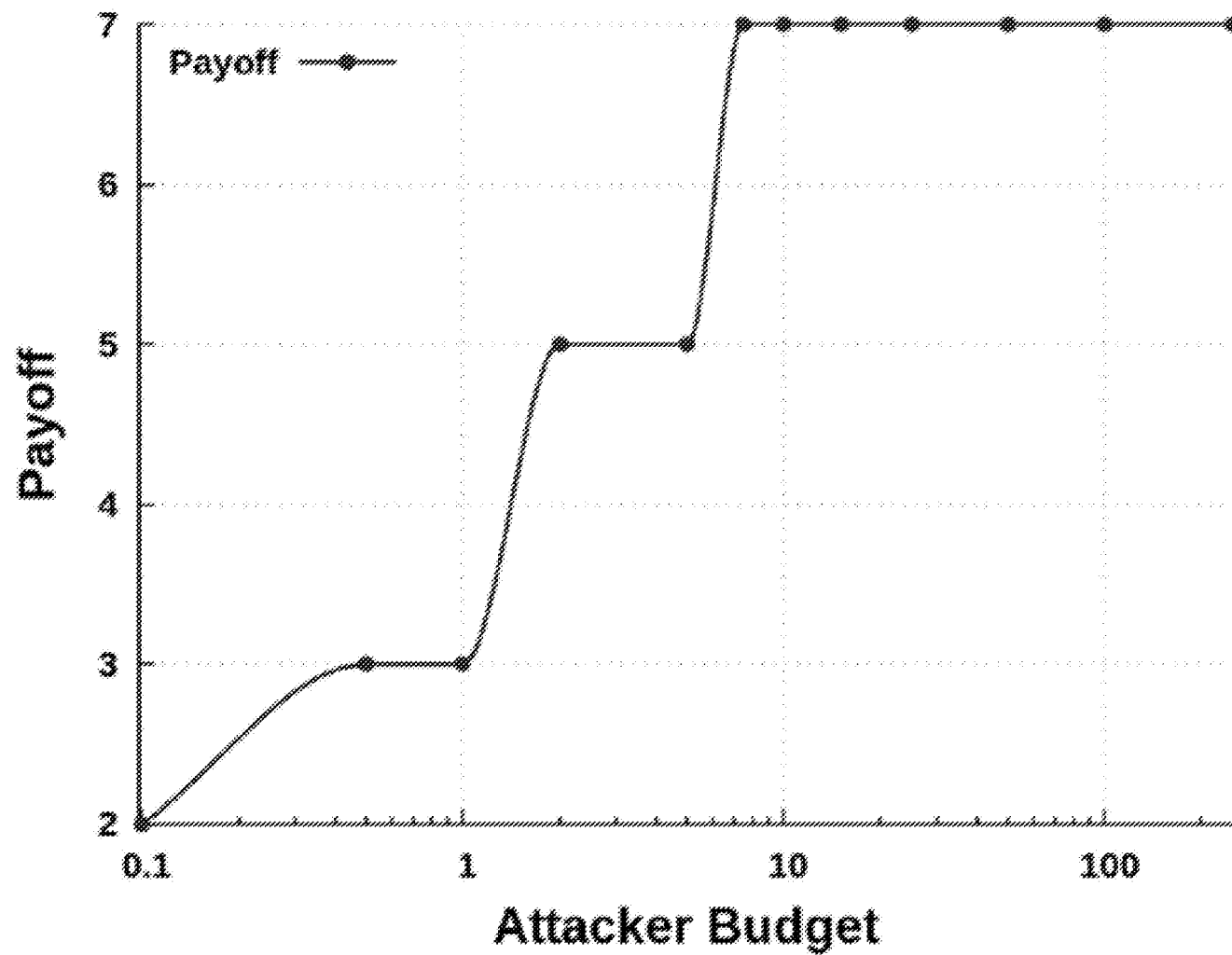


Fig. 4B

500

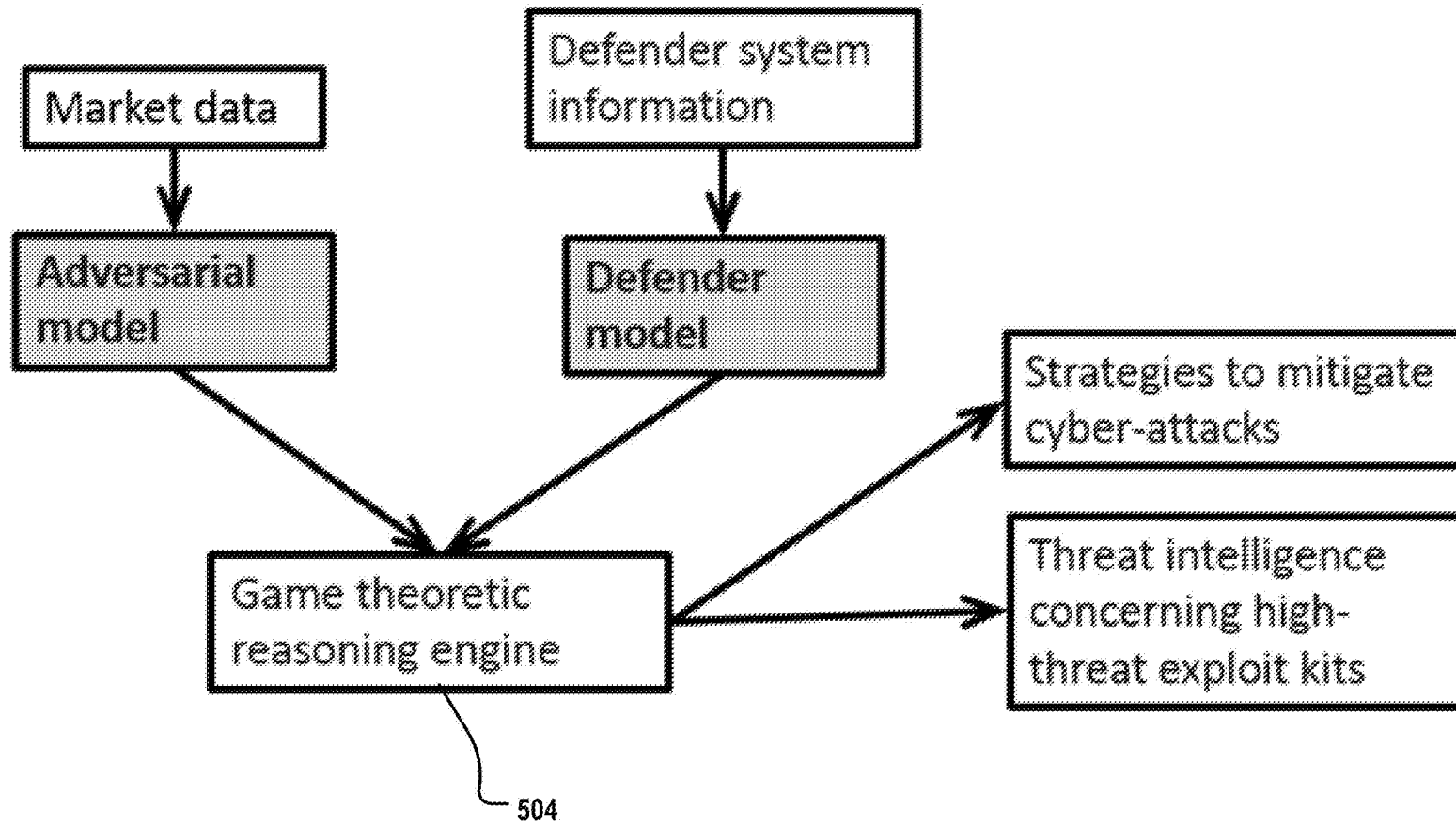
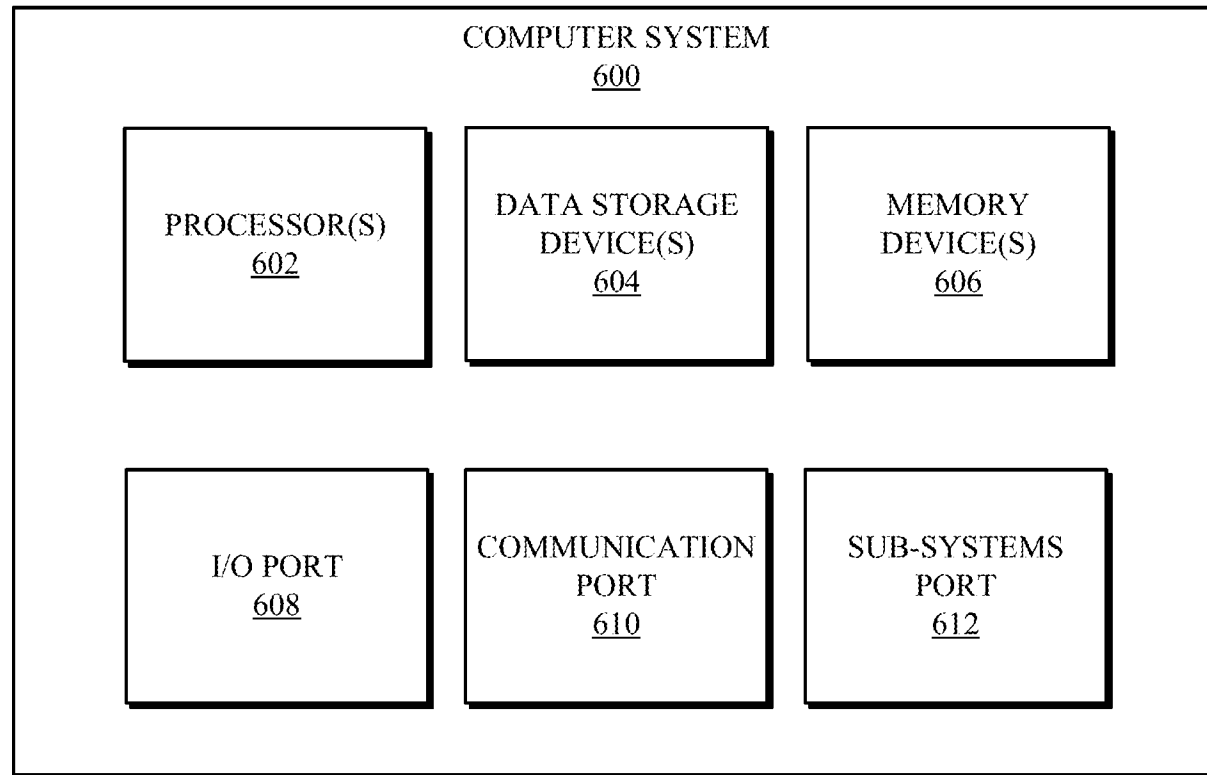


Fig. 5

**FIG. 6**

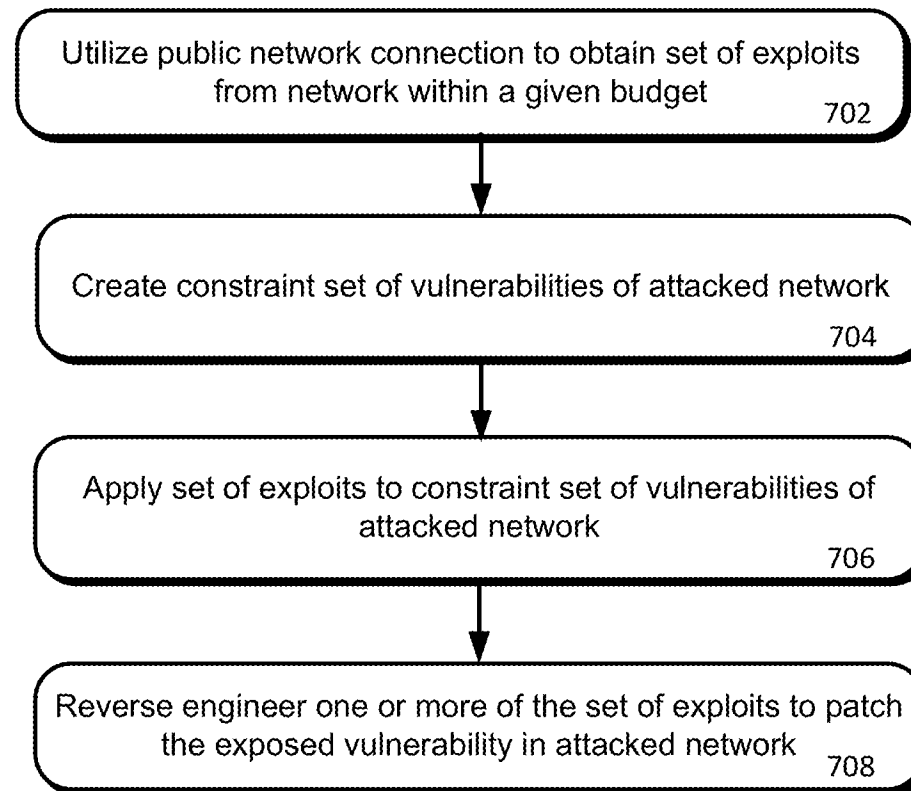
700


FIG. 7

Electronic Patent Application Fee Transmittal

Application Number:	15362730			
Filing Date:	28-Nov-2016			
Title of Invention:	SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION			
First Named Inventor/Applicant Name:	Paulo Shakarian			
Filer:	Ari M. Bai/Sam Bethune			
Attorney Docket Number:	055743-555439			
Filed as Micro Entity				
Filing Fees for Utility under 35 USC 111(a)				
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(\$)
Extension - 1 month with \$0 paid	3251	1	50	50
Miscellaneous:				
Total in USD (\$)				50

Electronic Acknowledgement Receipt

EFS ID:	35170597
Application Number:	15362730
International Application Number:	
Confirmation Number:	5936
Title of Invention:	SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION
First Named Inventor/Applicant Name:	Paulo Shakarian
Customer Number:	27148
Filer:	Ari M. Bai/Sam Bethune
Filer Authorized By:	Ari M. Bai
Attorney Docket Number:	055743-555439
Receipt Date:	15-FEB-2019
Filing Date:	28-NOV-2016
Time Stamp:	17:24:19
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	\$50
RAM confirmation Number	021919INTEFSW00004519501662
Deposit Account	
Authorized User	

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

IPR2025-01397

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment Copy Claims/Response to Suggested Claims	Response.pdf	63068	no	12
			3585e24baa03c3754779e8e7522964556eb376eb		
Warnings:					
Information:					
2	Drawings-only black and white line drawings	Drawings_Replacement_Sheet s.pdf	1812721	no	9
			15566a507cb73f27a3e2b4cb0611245bda3a72d6		
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30830	no	2
			37d5981b3f7589df2ce2ebbcdf137d05d339627d		
Warnings:					
Information:					
Total Files Size (in bytes):			1906619		
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.					

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Paulo Shakarian

Examiner: Henry Tsang

Serial No.: 15/362,730

Group Art Unit: 2495

Filed: November 28, 2016

Confirmation No.: 5936

For: SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER
THREAT MITIGATION

AMENDMENT & RESPONSE UNDER 37 C.F.R. §1.111

TO THE COMMISSIONER FOR PATENTS

Sir:

This paper is responsive to the non-final Office Action mailed on October 15, 2018. Please enter the following amendments and consider the remarks below in accordance with the Rules of Practice.

No fees are believed to be due in connection with the filing of this paper; however, should any fees be deemed necessary, the commissioner is hereby authorized to deduct any such fees from **Deposit Account No. 50-1662** referencing the above docket number.

Amendments to the claims are reflected in the listing that begins at page 2 of this paper.

Remarks begin at page 7 of this paper.

CLAIM AMENDMENTS

Please amend the claims as follows:

1. (Original) A system for protecting a computer system from attack, the system comprising:

a network connection ~~for communicating with a public network~~;

a processing device; and

a non-transitory computer-readable medium connected to the processing device

configured to store instructions that, when executed by the processing device, performs the operations of:

accessing data through the network connection, the data comprising dark net information associated with exploits of a computer system, comprising:

obtaining a set of exploits from the dark net information ~~public network through the network connection~~, the set of exploits configured to penetrate the computer system;

applying an exploit function which takes the set of exploits as input and returns a set of vulnerabilities;

creating a constraint set ~~of vulnerabilities~~ of the computer system from the set of vulnerabilities, the constraint set comprising a minimum set of

dependencies to operate the computer system;

applying the set of exploits to the computer system;

analyzing the application of the set of exploits on the computer system to detect a particular vulnerability of the computer system; and

altering a configuration of the computer system in response to the analysis of the application of the set of exploits to reduce potential damage of a cyberattack.

2. (Original) The system of claim 1, wherein analyzing the application of the set of exploits on the computer system comprises quantifying a risk level posed to the computer system related to a cost to obtain the set of exploits.
3. (Currently amended) The system of claim 2, wherein ~~the public network is the Internet and~~ the processing device further performs the operation of:
aligning Internet data with the constraint set of vulnerabilities based on information obtained about the set of exploits.
4. (Currently amended) The system of claim 3, wherein obtaining a set of exploits ~~from the public network~~ through the network connection comprises:
applying one or more algorithms to obtain the set of exploits ~~based on the constraint set of vulnerabilities of the computer system from one or more darknet marketplaces on the Internet.~~
5. (Original) The system of claim 4, wherein the one or more algorithms determine the cost to obtain the set of exploits to create a budget and obtains the set of exploits constrained by the determined cost to obtain the set of exploits.
6. (Original) The system of claim 5, wherein obtaining the set of exploits is based on maximizing the quantifying of the risk level posed to the computer system related to the cost to obtain the set of exploits.
7. (Original) The system of claim 1, wherein altering the configuration of the computer system comprises removing a software component of the computer system that is utilized by the set of exploits to attack the computer system.

8. (Currently amended) A method for improving a computing device, the method comprising:
- accessing data comprising dark net information associated with a computer system;
 - obtaining a set of exploits from the dark net information ~~a public network~~, the set of exploits configured to bypass a security feature of the computer system;
 - applying an exploit function which takes the set of exploits as input and returns a set of vulnerabilities;
 - analyzing an application associated with ~~[[of]]~~ the set of exploits on the computer system to detect a particular vulnerability of the set of vulnerabilities of the computer system; and
 - altering a configuration of the computer system in response to the analysis of the application of the set of exploits to reduce potential damage of a cyberattack.
9. (Original) The method of claim 8 further comprising:
- creating a constraint set of vulnerabilities of the computer system comprising a minimum set of dependencies to operate the computer system; and
 - wherein the application of the set of exploits on the computer system comprises determining the effect of the set of exploits on the constraint set of vulnerabilities of the computer system.
10. (Currently amended) The method of claim 9, wherein analyzing the application of the set of exploits on the computer system comprises quantifying a risk level posed to the computer system related to a cost to obtain the set of exploits ~~from the public network.~~
11. (Canceled)

12. (Currently amended) The method of claim 11, wherein obtaining a set of exploits ~~from the public network~~ comprises:
applying one or more algorithms to obtain the set of exploits based on the constraint set of vulnerabilities of the computer system from one or more darknet marketplaces on the Internet.
13. (Original) The method of claim 12, wherein the one or more algorithms determine the cost to obtain the set of exploits to create a budget and obtains the set of exploits constrained by the determined cost to obtain the set of exploits.
14. (Original) The method of claim 13, wherein obtaining the set of exploits is based on maximizing the quantifying of the risk level posed to the computer system related to the cost to obtain the set of exploits.
15. (Original) The method of claim 8, wherein altering the configuration of the computer system comprises removing a software component of the computer system that is utilized by the set of exploits to attack the computer system.
16. (Original) The method of claim 8, wherein altering the configuration of the computer system comprises installing a patch to a software component of the computer system that is exposed by the set of exploits to attack the computer system.
17. (Currently amended) One or more non-transitory tangible computer-readable storage media storing computer-executable instructions for performing a computer process on a machine, the computer process comprising:
obtaining a set of exploits from dark net information ~~a public network~~, the set of exploits configured to bypass a security feature of the computer system;

analyzing an application of the set of exploits on the computer system to detect a particular vulnerability of the computer system; and altering a configuration of the computer system in response to the analysis of the application of the set of exploits to reduce potential damage of a cyberattack.

18. (Original) The one or more non-transitory computer-readable storage media of claim 17, wherein the computer process further comprises:
 - creating a constraint set of vulnerabilities of the computer system comprising a minimum set of dependencies to operate the computer system; and
 - wherein the application of the set of exploits on the computer system comprises determining the effect of the set of exploits on the constraint set of vulnerabilities of the computer system.
19. (Currently amended) The one or more non-transitory computer-readable storage media of claim 17, wherein analyzing the application of the set of exploits on the computer system comprises quantifying a risk level posed to the computer system related to a cost to obtain the set of exploits ~~from the public network.~~
20. (Currently amended) The one or more non-transitory computer-readable storage media of claim 17, wherein obtaining a set of exploits ~~from the public network~~ comprises applying one or more algorithms to obtain the set of exploits from one or more darknet marketplaces on the Internet.

REMARKS

This paper responds to the Examiner's Non-Final Office Action mailed on October 15, 2018. Reconsideration and continued examination in view of the foregoing response is respectfully requested.

Status of Claims

Claims 1-20 were originally filed in the instant application, with claims 1, 8, and 17 being independent. By the present document, claims 1–10 and 12–20 are now pending, with claims 1, 8, and 17 being independent. Claim 11 has been cancelled. Claims 3, 4, 8, 10, 12, 17, 19, and 20 have been amended. No new subject matter has been added.

Drawings Objections

The Office Action objects to the drawings based on missing reference umbers. In response the Applicants present herewith replacement sheets for the drawings to notate the reference numbers identified by the Examiner as being absent from the drawings.

Claims Objections

The Office Action objects to the drawings based on the language of a computer-readable medium and the Applicants have amended this term to recite a “non-transitory computer-readable medium.”

§101 Rejections

The Examiner rejected claims 1-20 under U.S.C. Section 101 because the claimed invention is allegedly directed to a judicial exception (i.e., a law of nature, a natural phenomenon, or an abstract idea) without significantly more. Applicants respectfully traverse these rejections.

Section 101 of the Patent Act establishes that “[w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any

new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.” 35 U.S.C. §101. **The claims as presently amended are directed to improvements in cyber security using a novel framework for addressing penetration testing that is fed with real-world exploit market data, mined from the darknet.**

More particularly, as presently amended, independent claim 1 recites the claim features of:

a computer-readable medium connected to the processing device configured to store instructions that, when executed by the processing device, performs the operations of:

accessing data through the network connection, the data comprising dark net information associated with exploits of a computer system, comprising:
obtaining a set of exploits from the dark net information, the set of exploits configured to penetrate the computer system;
applying an exploit function which takes the set of exploits as input and returns a set of vulnerabilities;
creating a constraint set of the computer system from the set of vulnerabilities, the constraint set comprising a minimum set of dependencies to operate the computer system . . .
applying the set of exploits to the computer system;
analyzing the application of the set of exploits on the computer system to detect a particular vulnerability of the computer system; and
altering a configuration of the computer system in response to the analysis of the application of the set of exploits to reduce potential damage of a cyberattack.

Independent claims 8 and 17 as presently amended recite similar features.

The Applicants submit the subject matter of these newly amended claims is within one of the enumerated statutory classes. Accordingly, the Office bears the burden of making a *prima facie* case of unpatentability by showing that the claimed subject matter falls within one of the exceptions to statutory subject matter. *See Alice Corp. Pty. Ltd. v. CLS Bank Int’l*, 134 S. Ct. 2347, 2354 (2014); *In re Bilski*, 130 S.Ct. 3218 (2010); MPEP § 2106.

To meet this burden, the Office *must* present *supporting evidence* that the claims are directed to ineligible subject matter to satisfy the first prong of the *Alice* test for maintaining subject matter rejections under 101. *Alice*, 134 S.Ct. at 2355. Further, even if the Office demonstrates that the claims are directed to an abstract idea, the Office must satisfy the second prong of the *Alice* test and has the burden of providing evidence that the claim as a whole, including all elements or combination of elements, is not directed to significantly more than the abstract idea itself. *Id.*

In addition, the USPTO recently released the following updated information.

USPTO Updated 101 Instructions

The USPTO recently released a set of further instructions entitled, “2019 Revised Patent Subject Matter Eligibility Guidance” (hereinafter “Revised Instructions”). These Revised Instructions:

- define three categories of subject matter the Office deems to be abstract ideas: (1) mathematical concepts, (2) certain methods of organizing human activity, and (3) mental processes; and
- states that where a claim integrates a recited judicial exception (e.g., abstract idea) into a practical application of that exception, the claim is **not** “directed to” to a judicial exception, and is patent eligible.

Respectfully, the Applicant submits the Office Action does not meet the burden or requirements to show that the claimed subject matter is directed to a judicial exception, especially in view of the present amendments to the claims, and the 101 rejections must therefore be withdrawn. As set forth herein, the claims have been amended to clarify that data is accessed through the dark net. The claims have further been amended to clarify that a set of exploits is obtained from the dark net information, and then an exploit function is implemented to return a set of vulnerabilities. The claims further clarify that the claimed subject matter is implemented to reduce potential damage of a cyberattack. The Applicant submits these claim amendments clarify that any recitation of an alleged judicial exception in the claims is integrated into a practical application of that exception.

The claims do not simply recite the recitation of a mathematical concept or mental process. To the contrary, the claims recite a **practical application** of e.g., an exploit function to alter a configuration of a computer system in response to the analysis of the application of the set of exploits, in order to reduce potential damage of a cyberattack. Further, as discussed in, e.g., paragraphs [0055]-[0058] of the subject application, the claims recite an improvement in technology associated with cyber security including threat mitigation and response.¹

Moreover, the Applicants submit that the present claim amendments satisfy the machine or transformation test, which is sufficient for showing “significantly more” than any abstract idea allegedly recited within the claimed methods.

For at least the reasons set forth above, the Applicant respectfully requests the 101 rejections be withdrawn.

§103 Rejections (Norman, Wolff, Martinez)

The Examiner rejected claims 1, 7-9 and 15-18 under pre-AIA 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Application Publication No. 2004/0088565 to Norman et al. (“Norman”), in view of U.S. Patent Application Publication No. 2013/0198848 to Wolff (“Wolff”) and U.S. Patent Application Publication No. 2014/0137257 to Martinez et al. (“Martinez”). The Examiner further rejected claim 2-6, 9-14, 19 and 20 under pre-AIA 35 U.S.C. §103(a) as being unpatentable over Norman in view of Wolff and Martinez, and further in view of the article titled “International Vulnerability Purchase Program” by Frei et al. (“Frei”). Applicants respectfully traverse this rejection.

As set forth above, independent claim 1 as presently amended recites the following claim features:

accessing data through the network connection, the data comprising dark net information associated with exploits of a computer system, comprising:

¹ As set forth in MPEP 2106.05(a), claims that recite improvements to the functioning of a computer or to any other technology or technical field must be found patent eligible under Section 101.

obtaining a set of exploits from the dark net information, the set of exploits configured to penetrate the computer system;
applying an exploit function which takes the set of exploits as input and returns a set of vulnerabilities;
creating a constraint set of the computer system from the set of vulnerabilities, the constraint set comprising a minimum set of dependencies to operate the computer system . . .
applying the set of exploits to the computer system;
analyzing the application of the set of exploits on the computer system to detect a particular vulnerability of the computer system; and
altering a configuration of the computer system in response to the analysis of the application of the set of exploits to reduce potential damage of a cyberattack.

Independent claims 8 and 17 as presently amended recite similar features.

The claims have been amended to clarify that data is accessed through the dark net. The claims have further been amended to clarify that a set of exploits is obtained from the dark net information, and then an exploit function is implemented to return a set of vulnerabilities. The claims further clarify that the claimed subject matter is implemented to reduce potential damage of a cyberattack. The Applicants respectfully submit that the Norman, Wolff, and Martinez references fail to disclose alone or in combination all of the features of claim 1 as presently amended.

Accordingly, the Applicants respectfully request the 103 rejections be withdrawn.

CONCLUSION

By the present response, the Applicants respectfully submit that the claims are in a condition for allowance, and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicants' representative at (602) 650-2061 to facilitate prosecution of this application. If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 50-1662.

Respectfully submitted,

POLSINELLI PC

Date: February 15, 2019

By: /Ari M. Bai/
Ari M. Bai, Reg. No.: 38,726
One E. Washington Street, Suite 1200
Phoenix, AZ 85004
Direct Phone: (602) 650-2061
E-Mail: uspto@polsinelli.com
Attorney for Applicants

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 15/362,730		Filing Date 11/28/2016		☐ To be Mailed	
ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO									
APPLICATION AS FILED - PART I									
		(Column 1)	(Column 2)						
FOR		NUMBER FILED	NUMBER EXTRA		RATE (\$)		FEE (\$)		
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))		N/A	N/A		N/A				
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))		N/A	N/A		N/A				
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))		N/A	N/A		N/A				
TOTAL CLAIMS (37 CFR 1.16(i))		minus 20 = *		x \$80 =					
INDEPENDENT CLAIMS (37 CFR 1.16(h))		minus 3 = *		x \$420 =					
☐ 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).							
☐ 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				
APPLICATION AS AMENDED - PART II									
		(Column 1)		(Column 2)	(Column 3)				
AMENDMENT	02/15/2019	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	x \$100 =		0	
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0	x \$460 =		0	
	☐ Application Size Fee (37 CFR 1.16(s))								
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
						TOTAL ADD'L FEE		0	
		(Column 1)		(Column 2)	(Column 3)				
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	*	Minus	**	=	x \$0 =			
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x \$0 =			
	☐ Application Size Fee (37 CFR 1.16(s))								
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
						TOTAL ADD'L FEE			
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.						LIE			
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".						/DORIS M KING/			
*** 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.									

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

27148 7590 03/26/2019
POLSINELLI PC
900 WEST 48TH PLACE
SUITE 900
KANSAS CITY, MO 64112-1895

EXAMINER	
TSANG, HENRY	
ART UNIT	PAPER NUMBER
2495	

DATE MAILED: 03/26/2019

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/362,730	11/28/2016	Paulo Shakarian	055743-555439 M16-040P	5936

TITLE OF INVENTION: SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	MICRO	\$250	\$0.00	\$0.00	\$250	06/26/2019

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 ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

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: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (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)

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.

27148 7590 03/26/2019
POL SINELLI PC
900 WEST 48TH PLACE
SUITE 900
KANSAS CITY, MO 64112-1895

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 transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/362,730	11/28/2016	Paulo Shakarian	055743-555439 M16-040P	5936

TITLE OF INVENTION: SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	MICRO	\$250	\$0.00	\$0.00	\$250	06/26/2019

EXAMINER	ART UNIT	CLASS-SUBCLASS
TSANG, HENRY	2495	726-025000

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 03-09 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,

1 _____

(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.

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 must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). 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. Fees submitted: ☐ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

☐ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. Change in Entity Status (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____



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.
15/362,730	11/28/2016	Paulo Shakarian	055743-555439 M16-040P	5936
27148	7590	03/26/2019	EXAMINER	
POL SINELLI PC			TSANG, HENRY	
900 WEST 48TH PLACE			ART UNIT	
SUITE 900			PAPER NUMBER	
KANSAS CITY, MO 64112-1895			2495	

DATE MAILED: 03/26/2019

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

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

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.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B 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 30 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.

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) 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 of a Federal, State, or local law.

Notice of Allowability	Application No. 15/362,730	Applicant(s) Shakarian et al.	
	Examiner HENRY TSANG	Art Unit 2495	AIA (FITF) Status Yes

-- 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 02/15/2019.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

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 See Continuation Sheet. As a result of the allowed claim(s), 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**.

4. ☐ 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)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file areply 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. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ 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).

6. ☐ 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. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____. 3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____. 4. ☒ Interview Summary (PTO-413), Paper No./Mail Date. <u>03/07/2019</u> .	5. ☒ Examiner's Amendment/Comment 6. ☒ Examiner's Statement of Reasons for Allowance 7. ☐ Other _____.
--	---

Continuation of 3. The allowed claim(s) is/are: 1-8,10,12-17 and 19-20

DETAILED ACTION

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Timothy Fontes on 03/07/2019.

By this examiner's amendment Claims 1, 8, 10, 12 and 17 have been amended, and Claims 9 and 18 have been canceled as the following:

1. (Currently amended) A system for protecting a computer system from attack, the system comprising:
 - a network connection;
 - a processing device; and
 - a non-transitory computer-readable medium connected to the processing device configured to store instructions that, when executed by the processing device, performs the operations of:
 - accessing data through the network connection, the data comprising dark net information associated with exploits of a computer system, comprising:
 - obtaining a set of exploits from the dark net information, the set of exploits configured to penetrate the computer system;
 - applying an exploit function which takes the set of exploits as input and returns a set of vulnerabilities;
 - creating a constraint set of the computer system from the set of vulnerabilities, the constraint set comprising a minimum set of dependencies to operate the computer system;
 - applying the set of exploits to the constraint set of the computer system;

analyzing the application of the set of exploits on the computer system to detect a particular vulnerability of the computer system; and altering a configuration of the computer system in response to the analysis of the application of the set of exploits to reduce potential damage of a cyberattack.

8. (Currently amended) A method for improving a computing device, the method comprising:
 - accessing data comprising dark net information associated with a computer system;
 - obtaining a set of exploits from the dark net information, the set of exploits configured to bypass a security feature of the computer system;
 - applying an exploit function which takes the set of exploits as input and returns a set of vulnerabilities;
 - creating a constraint set of vulnerabilities of the computer system from the set of vulnerabilities comprising a minimum set of dependencies to operate the computer system, wherein application of the set of exploits on the computer system comprises determining the effect of the set of exploits on the constraint set of vulnerabilities of the computer system;
 - analyzing an application associated with the set of exploits on the computer system to detect a particular vulnerability of the constraint set of vulnerabilities of the computer system; and
 - altering a configuration of the computer system in response to the analysis of the application of the set of exploits to reduce potential damage of a cyberattack.
9. (Canceled)
10. (Currently amended) The method of claim ~~9~~ 8, wherein analyzing the application of the set of exploits on the computer system comprises quantifying a risk level posed to the computer system related to a cost to obtain the set of exploits.
12. (Currently amended) The method of claim ~~11~~ 10, wherein obtaining a set of exploits comprises:
 - applying one or more algorithms to obtain the set of exploits based on the constraint set of vulnerabilities of the computer system from one or more darknet marketplaces on the Internet.
17. (Currently amended) One or more non-transitory tangible computer-readable storage media storing computer-executable instructions for performing a computer process on a machine, the computer process comprising:

obtaining a set of exploits from dark net information, the set of exploits configured to bypass a security feature of ~~[[the]]~~ a computer system;
applying an exploit function which takes the set of exploits as input and returns a set of vulnerabilities;
creating a constraint set of vulnerabilities of the computer system from the set of vulnerabilities comprising a minimum set of dependencies to operate the computer system;
applying the set of exploits to the constraint set of vulnerabilities of the computer system;
analyzing ~~[[an]]~~ the application of the set of exploits on the computer system to detect a particular vulnerability of the computer system; and
altering a configuration of the computer system in response to the analysis of the application of the set of exploits to reduce potential damage of a cyberattack.

18. (Canceled)

Allowable Subject Matter

Claims 1-8, 10, 12-17, 19 and 20 are allowed.

Reasons for Allowance

Examiner's statement of reasons for allowance for claims 1-8, 10, 12-17, 19 and 20 are stated below.

Regarding independent Claims 1, 8 and 17, the Examiner found neither prior art cited in its entirety, nor based on the prior art, found any motivation to combine any of said prior art that teaches "obtaining a set of exploits from the dark net information, the set of exploits configured to penetrate the computer system; applying an exploit function which takes the set of exploits as input and returns a set of vulnerabilities; creating a constraint set of the computer system from the set of vulnerabilities, the constraint set comprising a minimum set of dependencies to operate the computer system; applying the set of exploits to the constraint set of the computer system; analyzing the application of the set of exploits on the computer system to detect a particular vulnerability of the computer system; and altering a configuration of the computer system in response to the analysis of the application of the set of exploits to

reduce potential damage of a cyberattack” in combination with all the elements of the independent claims respectively.

The dependent claims 2-7, 10, 12-16, 19 and 20 are allowable due to their dependence on independent claims 1, 8 and 17 respectively.

The closest prior art made of record are:

Norman (US2004/0088565) teaches a system and method for identifying a software vulnerability on a computer system. Applying an interrogation program to the software, the interrogation program being capable of exploiting a known software vulnerability if it is present in the software to which the interrogation program is applied; in the event that the software vulnerability is exploited by the interrogation program, operating the interrogation program to generate a set of management information from which can be derived the identification of the computer system; and sending the management information to the management system.

Martinez et al. (US2014/0137257) teaches a system and method for assessing a risk of one or more assets within an operational technology infrastructure by providing a database containing data relating to the one or more assets, calculating a threat score for the one or more assets using one or more processors communicably coupled to the database, calculating a vulnerability score for the one or more assets, calculating an impact score for the one or more assets, and determining the risk of the one or more assets based on the threat score, the vulnerability score and the impact score.

Wolff (US2013/0198848) teaches a method and system for vulnerability remediation. A CSVRS client includes software having a security vulnerability, which vulnerability may be known to malicious actors who develop an exploit. A RSP receives information about the exploit and vulnerability from a team of remediation experts. The RSP may prepare a remedial exploit, which carries a self-healing payload. The remedial exploit may be delivered either through the vulnerability itself, or through credentials granted by the CSVRS client to the RSP. The self-healing payload takes appropriate action, such as closing ports or disabling scripts, to prevent the vulnerability from being further exploited.

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

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HENRY TSANG whose telephone number is (571)270-7959. The examiner can normally be reached on M-F 8am - 5pm EST.

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 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.

/HENRY TSANG/
Primary Examiner, Art Unit 2495

<i>Search Notes</i> 	Application/Control No. 15/362,730	Applicant(s)/Patent Under Reexamination Shakarian et al.
	Examiner HENRY TSANG	Art Unit 2495

CPC - Searched*		
Symbol	Date	Examiner
H04L63/1433 keywords	10/10/2018	HT
H04L63 keywords	10/10/2018	HT
H04L63 keywords	03/07/2019	HT

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Inventer/Assignee search in EAST	10/10/2018	HT
EAST text search with keywords	10/10/2018	HT
Inventer/Assignee search in EAST	03/07/2019	HT
EAST text search with keywords	03/07/2019	HT
Google search with keywords	03/07/2019	HT

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
H04L63	keywords	10/10/2018	HT
H04L63	keywords	03/07/2019	HT

/HENRY TSANG/ Primary Examiner, Art Unit 2495	
--	--

<i>Search Notes</i> 	Application/Control No. 15/362,730	Applicant(s)/Patent Under Reexamination Shakarian et al.
	Examiner HENRY TSANG	Art Unit 2495

/HENRY TSANG/ Primary Examiner, Art Unit 2495	
--	--

<i>Issue Classification</i> 	Application/Control No. 15/362,730	Applicant(s)/Patent Under Reexamination Shakarian et al.
	Examiner HENRY TSANG	Art Unit 2495

CPC						
Symbol					Type	Version
H04L	/	63	/	1433	F	2013-01-01
H04L	/	63	/	1441	I	2013-01-01
G06Q	/	30	/	0201	I	2013-01-01

CPC Combination Sets				
Symbol		Type	Set	Ranking
	/			

NONE (Assistant Examiner) _____ (Date) _____		Total Claims Allowed: 17	
/HENRY TSANG/ Primary Examiner, Art Unit 2495 (Primary Examiner) _____ (Date) 08 March 2019		O.G. Print Claim(s) 1	O.G. Print Figure 7

<i>Issue Classification</i> 	Application/Control No. 15/362,730	Applicant(s)/Patent Under Reexamination Shakarian et al.
	Examiner HENRY TSANG	Art Unit 2495

INTERNATIONAL CLASSIFICATION			
CLAIMED			
H04L	/	29	/ 06
NON-CLAIMED			
/		/	

US ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS

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

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	17	
/HENRY TSANG/ Primary Examiner, Art Unit 2495	08 March 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	7

Issue Classification 	Application/Control No. 15/362,730	Applicant(s)/Patent Under Reexamination Shakarian et al.
	Examiner HENRY TSANG	Art Unit 2495

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47															
CLAIMS															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	9	10	16	19										
2	2		11	17	20										
3	3	10	12												
4	4	11	13												
5	5	12	14												
6	6	13	15												
7	7	14	16												
8	8	15	17												
	9		18												

NONE (Assistant Examiner) _____ (Date) _____		Total Claims Allowed: 17	
/HENRY TSANG/ Primary Examiner, Art Unit 2495 (Primary Examiner) _____ (Date) 08 March 2019		O.G. Print Claim(s) 1	O.G. Print Figure 7

EAST Search History (Prior Art)

IPR2025-01397

			BM_TDB			
--	--	--	--------	--	--	--

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S125	1	h04l63\$.cpc. and ((exploit or vulnerab\$5) and budget and cost and (darknet or black\$2market)).clm.	US-PGPUB; USPAT	ADJ	ON	2019/03/07 16:22
S126	1	((exploit or vulnerab\$5) and budget and cost and (darknet or black\$2market)).clm.	US-PGPUB; USPAT	ADJ	ON	2019/03/07 16:22
S127	1	((exploit or vulnerab\$5) and risk and cost and (darknet or black\$2market)).clm.	US-PGPUB; USPAT	ADJ	ON	2019/03/07 16:22

3/ 8/ 2019 1:47:09 PM
C:\ Users\ htsang\ Documents\ EAST\ Workspaces\ 15362730.w sp

Any time

Since 2019

Since 2018

Since 2015

Custom range...

Sort by relevance

Sort by date

☒ include patents

☒ include citations

☒ Create alert

The legitimate vulnerability **market**: Inside the secretive world of 0-day exploit sales

C Miller - In Sixth Workshop on the Economics of Information ..., 2007 - Citeseer
... have existed. A **black market** for these **exploits** has developed around their illegal use. Recently, a trend has developed toward buying and selling these **exploits** as a source of legitimate income for security researchers. However ...
Cited by 117 Related articles All 2 versions

Comparing vulnerability severity and **exploits** using case-control studies

L Alodi, E Massacci - ACM Transactions on Information and System ..., 2014 - dl.acm.org
... Our analysis is based on four datasets reporting data on vulnerabilities and CVSS scores, proof-of-concept **exploits**, **exploits** traded in the **black markets**, and **exploits** in ... **Black**-marketed **exploits** ... EKITS CVEs in the **black market** Ad-hoc analysis + Contagio's Exploit table 103 Fig ...
Cited by 71 Related articles All 9 versions

[PDF] unitn.it
Full-Text @ USPTO-STIC

Markets for zero-day **exploits**: Ethics and implications

S Egelman, C Herley, PC Van Oorschot - Proceedings of the 2013 New ..., 2013 - dl.acm.org
... March 15, 2013. <http://techliberation.com/2013/03/15/regulating-the-market-for-zero-day-exploits-look-to-the-demand-side/> [11] Andy Ozment. Bug auctions: Vulnerability **markets** reconsidered ...
'Zero-day' **black market**—Where hackers buy secrets to exploit tech flaws ...
Cited by 30 Related articles All 10 versions

[PDF] psu.edu
Full-Text @ USPTO-STIC

[PDF] Curbing the **market** for cyber weapons

PN Stockton, M Golabek-Goldman - Yale L. & Pol'y Rev., 2013 - HeinOnline
... the "Silk Road" website recently shut down by the FBI, are located on the underground "Deep Web" and concealed from traditional search engines." In between the white and anarchic **black markets** for Oday **exploits**, there is an unregulated, burgeoning gray **market**, where bona ...
Cited by 38 Related articles All 8 versions

[PDF] heinonline.org
Full-Text @ USPTO-STIC

Related searches

vulnerability black market

black market **economy**

black markets **survival in the siege**

labor market blacks and whites

black markets **blue helmets**

Shifts in the cybersecurity paradigm: Zero-day **exploits**, discourse, and emerging institutions

A Kuehn, M Mueller - Proceedings of the 2014 New Security Paradigms ..., 2014 - dl.acm.org
... Developing institutions that affect and influence the trade of software vulnerabilities and **exploits** fall into ... 3. VULNERABILITY **MARKETS** AS INSTI- TUTIONS This section reports briefly on a preliminary analysis of ... Notably, Microsoft attempts to target the **black market** with its BBP ...
Cited by 7 Related articles

Full-Text @ USPTO-STIC

The marginalization of **black** executives

SM Collins - Social Problems, 1989 - academic.oup.com
... The new **black** middle class grounded in jobs in private industry was not created merely by tight **markets** and supply factors, such as educational attainment ... Develops and **exploits** the **black** consumer **market**, ie, special **market** sales and advertising. Mainstream ...
Cited by 166 Related articles All 10 versions

[PDF] heinonline.org
Full-Text @ USPTO-STIC

Xbox 360 hoaxes, social engineering, and gamertag **exploits**
A Podhradsky, R D'Ovidio... - 2013 46th Hawaii ... , 2013 - [ieeexplore.ieee.org](#)
... tool, the hacker is capable of gaining access to another gamer's IP and MAC
addresses which
he then **exploits** to repeatedly ... to either steal Reaver95's identity, perform an extremely
sophisticated social engineering attack, or to sell his identity on the **black market** (Ferro, 2012) ...
Cited by 9 Related articles All 4 versions

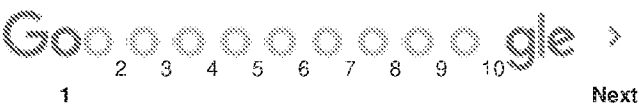
[PDF] computer.org
Full-Text @ USPTO-STIC

[book] **Markets** for cybercrime tools and stolen data: Hackers' bazaar
[L.Ablon](#), MC Libicki, AA Golay - 2014 - [books.google.com](#)
... the **market** for stolen infor- mation is very much alive and thriving, as is the **market** for the ... **Black**
markets are organized and run for the purpose of cybercrime;1 they deal in exploit kits ... Gray
markets, by our definition, are limited to the exchange of vulnerabilities and **exploits**, the dis ...
Cited by 180 Related articles All 6 versions

[book] Blue helmets and **black markets**: The business of
survival in the siege of Sarajevo
[P.Andreas](#) - 2011 - [books.google.com](#)
... of Mobility and Access The UN-Controlled Airport as Smuggling Hub Tunneling under the Siege:
Lifeline and Profit Center Trading with the Enemy The Media and Its Dependence on the **Black**
Market The Money Letter Smuggling System The Smugglers' **Markets** and Cigarettes ...
Cited by 210 Related articles All 5 versions

[doc] wilsoncenter.org

[book] Deviant globalization: **Black market** economy in the 21st century
[N.Gilman](#), J Goldhammer, S Weber - 2011 - [books.google.com](#)
... Introduction The **black market** was a way of getting around government controls ... unfet- tered
capitalism inevitably undermines the social and political foundations necessary to sustain **markets**.
More recently, Naomi Klein has contended that free **market** capitalism feeds ...
Cited by 88 Related articles All 2 versions





Any time

Since 2019

Since 2018

Since 2015

Custom range...

Sort by relevance

Sort by date

☒ include patents

☒ include citations

☒ Create alert

Darknet mining and game theory for enhanced cyber threat intelligence

J Robertson, A Diab, [E Marin](#), [E Nunes](#), V Paliath... - The Cyber Defense ..., 2016 - JSTOR
... Li and Chen 2014), which did not focus on the **purchase** and sale of specific items ... We will use ex to denote a particular exploit—a technique used to take advantage of a given **vulnerability**. Let Ex denote the set of all possible **exploits** and Ex denote the set of all possible exploit ...
Cited by 3 Related articles

Data driven game theoretic cyber threat mitigation

[PDF] aaai.org

J Robertson, V Paliath, [J Shakaran](#), A Thant... - Twenty-Eighth IAAI .., 2016 - aaai.org
... Li and Chen 2014), which did not focus on the **purchase** and sale of specific items ... We will use ex to denote a particular exploit - a tech- nique used to take advantage of a given **vulnerability**. Let Ex denote the set of all possible **exploits** and Ex denote the set of all possible exploit ...
Cited by 11 Related articles All 2 versions

Malware Trends on 'Darknet' Crypto-Markets: Research Review

[PDF] researchgate.net

[R Broadhurst](#), D Lord, D Maxim... - Available at SSRN ..., 2018 - papers.ssrn.com
... and bitcoin mining to pay for the various costs involved such as **purchasing** cryptocurrencies, VPN ... providing opportunities to **purchase** potentially lucrative **exploits** ... In the current environment both cryptocurrencies and **purchases** of malware or other software vulnerabilities on the ...
Related articles All 4 versions

[PDF] Anatomy of a Crime: Secure DevOps or Darknet Early Breach Detection

[PDF] usenix.org

[S Cortes](#) - 2018 - usenix.org
... stores • Resell fraudulently **purchased** goods on the internet ... 24 - April 2013 • Password Cracking; Account acquisition from the **darknet** July 2013 • Zero-day Attack: Exploit **vulnerability** • Jump the barriers between vendor and retailer system Page 25 ...
All 2 versions

Data Driven Game Theoretic Cyber Threat Mitigation

[P Shakaran](#) - pdfs.semanticscholar.org
... Less Expensive -- This method offers an alternative to **purchasing** zero-day **exploits** on the darkweb for penetration testing ... Therefore, a new approach is needed to understand which zero-day **exploits** an attacker will most likely **purchase** and how to defend against ...

D-miner: A framework for mining, searching, visualizing, and alerting on darknet events

[PDF] ieee.org
Full-Text @ USPTO-STIC

[H Lawrence](#), [A Hughes](#), R Tonic... - 2017 IEEE Conference ..., 2017 - ieeeexplore.ieee.org
... either through renting established botnets, **purchasing** malware source code, or **purchasing** guides to ... Knowledge of the frequency of **purchase** of different malware families provides a forward ... facets of darkweb data (eg, drug market globalization, weapons **purchases**) can also ...
Related articles All 3 versions

Systems and methods for data driven game theoretic cyber threat mitigation

[PDF] googleapis.com

[P Shakaran](#), J Robertson, [J Shakaran](#)... - US Patent App. 15 ..., 2017 - Google Patents
... an organization), the present disclosure models an attacker who, given a budget, will **purchase exploits** to maximize ... to denote a particular exploit—a technique used to take advantage of a given **vulnerability**. Let Ex denote the set of all possible **exploits** and Ex denote the set of ...
All 2 versions

What Is Vulnerability Assessment?

A Kakareka - Managing Information Security, 2013 - Elsevier
... Those offers provide a legitimate market for the **purchase** and sale of **vulnerability** ... What will happen if a **Vulnerability** is exploited and who **exploits** vulnerabilities ... "Vulnerability Assessment Scanning: Why Sunbelt Network Security Inspector (SNSI)?" Sunbelt Software, [http://img2 ...

IPR2025-01397

CrowdStrike EX1002 Page 152

Cited by 7 Related articles All 3 versions

[PDF] The network structure of opioid distribution on a **darknet** cryptomarket

[SW Duxbury, DL Haynie](#) - Journal of quantitative criminology, 2017 - Springer

... which buyers **purchased** from which vendors and how frequently buyers **purchased** from given ... we analyze is weighted by the frequency with which buyers **purchase** from specific ... of initial vendors, weighting the network by the frequency of buyers' **purchases** captures repeat ...

Cited by 7 Related articles All 4 versions

[PDF] [springer.com](#)
Full-Text @ USPTO-STIC

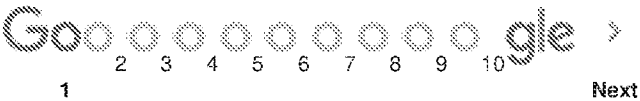
[PDF] **Darknets**, DRM, and trusted computing: Economic incentives for platform providers

[A Acquisti](#) - Workshop on Information Systems and ..., 2004 - [fabrice.rochelandet.free.fr](#)

... that, even if one DRM client is "broken," the same **vulnerability** cannot be used for all other DRM clients of the same type ... sending the decision of consumer i (not) to **purchase** good g . pg_A is the price ... enues come from the consumers' **purchases** of their platform. (For simplicity, 17 ...

Cited by 9 Related articles

[PDF] [free.fr](#)



Any time

Since 2019

Since 2018

Since 2015

Custom range...

Sort by relevance

Sort by date

☒ include patents

☒ include citations

☐ Create alert

State of the art: Automated black-box web application vulnerability testing

J Bau, E Bursztein, D Gupta... - 2010 IEEE Symposium ..., 2010 - ieeexplore.ieee.org

Black-box web application **vulnerability** scanners are automated tools that probe web applications for security vulnerabilities. In order to assess the current state of the art, we obtained access to eight leading tools and carried out a study of:(i) the class of ...

Cited by 297 Related articles All 23 versions

[PDF] Syntax-based Vulnerability Testing of Frame-based Network Protocols.

O Tai, S Knight, T Dean - PST, 2004 - Citeseer

Abstract Syntax-based **vulnerability testing** is a static black-box **testing** method for protocol implementations. It involves **testing** the Implementation Under Test (IUT) with a large number of mutated Protocol Data Units (PDUs), built by intentionally disobeying the protocol's ...

Cited by 66 Related articles All 7 versions

[HTML] Computerised physician order entry-related medication errors: analysis of reported errors and vulnerability testing of current systems

GD Schiff, MG Amato, T Equale, JJ Boehne ... - BMJ Qual ... , 2015 - qualitysafety.bmj.com

Importance Medication computerised provider order entry (CPOE) has been shown to decrease errors and is being widely adopted. However, CPOE also has potential for introducing or contributing to errors. Objectives The objectives of this study are to (a) analyse ...

Cited by 84 Related articles All 16 versions

Software security vulnerability testing in hostile environments

HH Thompson, JA Whittaker, FE Mottay - Proceedings of the 2002 ACM ..., 2002 - dl.acm.org

Traditional Black box software **testing** can be effective at exposing some classes of software failures. Security class failures, however, do not tend to manifest readily using these techniques. The problem is that many security failures occur in stressed environments ...

Cited by 49 Related articles All 2 versions

Related searches

vulnerability testing penetration

software vulnerability testing

security vulnerability testing

web application vulnerability testing

vulnerability testing model based

vulnerability testing black box

vulnerability testing defibrillation

vulnerability testing upper limit

[PDF] Vulnerability testing of software system using fault injection

W Du, AP Mathur - ... Lafayette, Indiana, Technique Report: COAST TR, 1993 - academia.edu

We describe an approach for **testing** a software system for possible security flaws. Traditionally, security **testing** is done using penetration analysis and formal methods. Based on the observation that most security flaws are triggered due to a flawed interaction with the ...

Cited by 45 Related articles All 9 versions

Model-based security vulnerability testing

PAP Salas, P Krishnan, KJ Ross - 2007 Australian Software ..., 2007 - ieeexplore.ieee.org

[PDF] ieee.org

Full-Text @ USPTO-STIC

[PDF] psu.edu

Full-Text @ USPTO-STIC

[HTML] bmj.com

Full-Text @ USPTO-STIC

[PDF] ieee.org

Full-Text @ USPTO-STIC

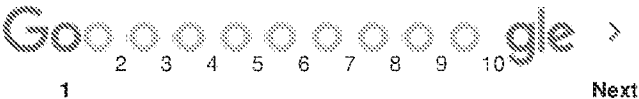
In this work we present a model-based framework for security vulnerabilities **testing**. Security vulnerabilities are not only related to security functionalities at the application level but are sensitive to implementation details. Thus traditional model-based approaches which elide ...
Cited by 37 Related articles All 4 versions

Model-based vulnerability testing for web applications [PDF] archives-ouvertes.fr
F Lebeau, B Legrand, E Patureux. ... on Software Testing ... 2013 -
ieeexplore.ieee.org Full-Text @ USPTO-STIC
This paper deals with an original approach to automate Model-Based **Vulnerability Testing** (MBVT) for Web applications, which aims at improving the accuracy and precision of **vulnerability testing**. Today, Model-Based **Testing** techniques are mostly used to address ...
Cited by 28 Related articles All 12 versions

[PDF] **BGP Vulnerability Testing: Separating Fact from FUD** [PDF] blackhat.com
v1.
S Convery, M Franz - NANOG28 Meeting 2003 and Black Hat USA ..., 2003 - blackhat.com
Victim# netstat-an| grep -tcp tcp 0 0 10.89. 168.101: 179 10.89. 168.99: 4189 SYN_RECV
tcp 0 0 10.89. 168.101: 179 10.89. 168.99: 8017 SYN_RECV tcp 0 0 10.89. 168.101: 179
10.89. 168.99: 56477 SYN_RECV tcp 0 0 10.89. 168.101: 179 10.89. 168.99: 41185 ...
Cited by 24 Related articles All 13 versions

[HTML] Nonprofit financial **vulnerability: Testing** competing [HTML] springer.com
models, recommended improvements, and implications Full-Text @ USPTO-STIC
E Teveli, H Katz, DM Brock - Voluntas: International Journal of Voluntary ..., 2015
- Springer
We examine the predictive validity of existing models used by researchers and by professional rating agencies of nonprofit organizations to assess financial **vulnerability**, on a sample of performing arts organizations. The models tested include Ohlson's (J Account Res ...
Cited by 33 Related articles All 9 versions

[BOOK] Metasploit toolkit for penetration **testing**, exploit development, and **vulnerability** research
D Maynor - 2011 - books.google.com
Metasploit Toolkit for Penetration **Testing**, Exploit Development, and **Vulnerability** Research is the first book available for the Metasploit Framework (MSF), which is the attack platform of choice for one of the fastest growing careers in IT security: Penetration **Testing**. The book will ...
Cited by 139 Related articles All 4 versions



PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (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)

27148 7590 03/26/2019
POL SINELLI PC
900 WEST 48TH PLACE
SUITE 900
KANSAS CITY, MO 64112-1895



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 via EFS-Web.

Rebecca L. Endsley, Paralegal (Typed or printed name)
/Rebecca L. Endsley/ (Signature)
04/02/2019 (Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/362,730	11/28/2016	Paulo Shakarian	055743-555439 M16-040P	5936

TITLE OF INVENTION: SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	MICRO	\$250	\$0.00	\$0.00	\$250	06/26/2019

EXAMINER	ART UNIT	CLASS-SUBCLASS
TSANG, HENRY	2495	726-025000

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 03-09 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.

POL SINELLI PC

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 must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Arizona Board of Regents on Behalf of Arizona State University Tempe, Arizona

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

4a. Fees submitted: ☒ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

☒ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 501662

5. Change in Entity Status (from status indicated above)

- ☐ Applicant certifying micro entity status. See 37 CFR 1.29
☐ Applicant asserting small entity status. See 37 CFR 1.27
☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Ari M. Bai/

Date 04/02/2019

Typed or printed name Ari M. Bai

Registration No. 38726

United States Patent and Trademark Office

- Sales Receipt -

04/03/2019 INTEFSW 00002104 15362730

01 FC:3501 250.00 DA

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (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)

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.

27148 7590 03/26/2019
POL SINELLI PC
900 WEST 48TH PLACE
SUITE 900
KANSAS CITY, MO 64112-1895

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited via EFS-Web.

Rebecca L. Endsley, Paralegal	(Typed or printed name)
/Rebecca L. Endsley/	(Signature)
04/02/2019	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/362,730	11/28/2016	Paulo Shakarian	055743-555439 M16-040P	5936

TITLE OF INVENTION: SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	MICRO	\$250	\$0.00	\$0.00	\$250	06/26/2019

EXAMINER	ART UNIT	CLASS-SUBCLASS
TSANG, HENRY	2495	726-025000

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 03-09 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.

POL SINELLI PC

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 must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Arizona Board of Regents on Behalf of Arizona State University Tempe, Arizona

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

4a. Fees submitted: ☒ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

☒ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 501662

5. Change in Entity Status (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Ari M. Bai/

Date 04/02/2019

Typed or printed name Ari M. Bai

Registration No. 38726

Electronic Patent Application Fee Transmittal

Application Number:	15362730			
Filing Date:	28-Nov-2016			
Title of Invention:	SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION			
First Named Inventor/Applicant Name:	Paulo Shakarian			
Filer:	Ari M. Bai/Rebecca Endsley			
Attorney Docket Number:	055743-555439 M16-040P			
Filed as Micro Entity				
Filing Fees for Utility under 35 USC 111(a)				
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 ISSUE FEE	3501	1	250	250

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				250

Electronic Acknowledgement Receipt

EFS ID:	35604739
Application Number:	15362730
International Application Number:	
Confirmation Number:	5936
Title of Invention:	SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION
First Named Inventor/Applicant Name:	Paulo Shakarian
Customer Number:	27148
Filer:	Ari M. Bai/Rebecca Endsley
Filer Authorized By:	Ari M. Bai
Attorney Docket Number:	055743-555439 M16-040P
Receipt Date:	02-APR-2019
Filing Date:	28-NOV-2016
Time Stamp:	15:29:40
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	\$ 250
RAM confirmation Number	040319INTEFSW00002104501662
Deposit Account	
Authorized User	

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

IPR2025-01397

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)	555439_Part_B_Fee_Transmittal.pdf	113612	no	1
			71b0813ac1c6c90aa16c1b38e77a6c96defa509e		
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30519	no	2
			7a8a0b0be04adc7049690c182939381240938195		
Warnings:					
Information:					
Total Files Size (in bytes):			144131		
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.
15/362,730	11/28/2016	Paulo Shakarian	055743-555439 M16-040P	5936
27148	7590	04/08/2019	EXAMINER	
POL SINELLI PC			TSANG, HENRY	
900 WEST 48TH PLACE				
SUITE 900				
KANSAS CITY, MO 64112-1895				
			ART UNIT	PAPER NUMBER
			2495	
			NOTIFICATION DATE	DELIVERY MODE
			04/08/2019	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):

patentdocketing@polsinelli.com
rendsley@polsinelli.com



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

Application No. : 15362730
Applicant : Shakarian
Filing Date : 11/28/2016
Date Mailed : 04/08/2019

NOTICE TO FILE CORRECTED APPLICATION PAPERS

Notice of Allowance Mailed

This application has been accorded an Allowance Date and is being prepared for issuance. The application, however, is incomplete for the reasons below.

Applicant is given two (2) months from the mail date of this Notice within which to respond. This time period for reply is extendable under 37 CFR 1.136(a) for only TWO additional MONTHS.

The informalities requiring correction are indicated in the attachment(s). If the informality pertains to the abstract, specification (including claims) or drawings, the informality must be corrected with an amendment in compliance with 37 CFR 1.121 (or, if the application is a reissue application, 37 CFR 1.173). Such an amendment may be filed after payment of the issue fee if limited to correction of informalities noted herein. See Waiver of 37 CFR 1.312 for Documents Required by the Office of Patent Publication, 1280 Off. Gaz. Patent Office 918 (March 23, 2004). In addition, if the informality is not corrected until after payment of the issue fee, for purposes of 35 U.S.C. 154(b)(1)(iv), “all outstanding requirements” will be considered to have been satisfied when the informality has been corrected. A failure to respond within the above-identified time period will result in the application being ABANDONED.

See attachment(s).

*A copy of this notice **MUST** be returned with the reply. Please address response to
“Mail Stop Issue Fee, Commissioner for Patents,
P.O. Box 1450, Alexandria, VA 22313-1450”.*

/Chris Harmon/
Publication Branch
Office of Data Management
(571) 272-4200

NON-COMPLIANT ILLUSTRATIONS IN SPECIFICATION OR CLAIMS

- ☒ The illustration(s) in the location(s) referenced below do not come within the exceptions of 37 CFR 1.58(a). Please delete the illustration(s) from the specification or claims, provided the illustration(s) as part of the formal drawing(s) in accordance with 37 CFR 1.84, and amend the specification to provide a brief description of the drawings in accordance with 37 CFR 1.74. Please see the following item(s):
- ☒ Specification document coded SPEC dated 11/28/2016, page(s) 15.
 - ☐ Claims document coded dated , claim(s) .
 - ☐ Amendment document coded dated .
 - ☐ Other: .
- ☐ The chemical formula(s), mathematical formula(s), or table(s) in the location(s) referenced below contain shading (color/grayscale) and therefore do not comply with 37 CFR 1.52 and do not come within the exceptions of 37 CFR 1.58(a). Please delete chemical formula(s), mathematical formula(s), or table(s) with shading from the specification or claims, provide them as formal color drawing(s) in accordance with 37 CFR 1.84, including petition, fee, and amendment in accordance with 37 CFR 1.84(a)(2), and amend the specification to provide a brief description of the drawings in accordance with 37 CFR 1.74. Please see the following item(s):
- ☐ Specification document coded dated , page(s) .
 - ☐ Claims document coded dated , claim(s) .
 - ☐ Amendment document coded dated .
 - ☐ Other: .

**IDENTIFICATION OF APPLICATION DEFICIENCIES
IN APPLICATION FILED ON OR AFTER SEPTEMBER 16, 2012**

- ☒ Applicant must provide legible text for the following item(s).
- ☒ Specification filed 11/28/2016, page(s) 3,8-13,15.
- ☐ Claims filed , claim(s) .
- ☐ Other: .
- ☐ Applicant must provide missing information on the following page(s) of the specification by amending the specification to add the missing text. No new matter may be added.
Page/line no(s).
- ☐ The specification refers to one or more applications by attorney docket number and does not show the U.S. application number(s). Applicant must supply the U.S. application number in place of each attorney docket number.
Page/line no(s).
- ☐ Applicant must provide an Abstract of the Disclosure.
- ☐ The Application Data Sheet (ADS dated) does not supply the inventor's city and/or does not supply the inventor's U.S. state and/or does not supply the inventor's country. Applicant must submit a signed, in accordance with 37 CFR 1.76(e) and 1.33(b), application data sheet that corrects this deficiency. To be in compliance with 37 CFR 1.76, the corrected application data sheet must identify the information being changed by using underlining for additions and strikethroughs or brackets for deletions.
- ☐ Other:

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Paulo Shakarian

Examiner: Henry Tsang

Serial No.: 16/362,730

Group Art Unit: 2495

Filed: November 28, 2016

Confirmation No.: 5936

For: SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER
THREAT MITIGATION**RESPONSE TO NOTICE TO FILE CORRECTED APPLICATION PAPERS
UNDER 37 C.F.R. §1.136(a)**

TO THE COMMISSIONER FOR PATENTS

Sir:

This paper is responsive to the Notice to File Corrected Application Papers mailed on April 8, 2019. Amendments to the specification are to correct minor typographical errors. The specification has been updated to provide legible text for tables, algorithms, and equations on pages 3, 8-13, and 15. Additionally, Applicant has attached hereto a Marked-Up Specification and a Substitute Specification. Applicant avers that no new matter has been introduced by virtue of these text clarifications.

No fees are believed to be due in connection with the filing of this paper; however, should any fees be deemed necessary, the Commissioner is hereby authorized to deduct any such fees from **Deposit Account No. 50-1662** referencing the above docket number.

Amendments to the Specification are reflected in the listing that begins at page 2 of this paper.

Remarks begin at page 4 of this paper.

AMENDMENTS TO THE SPECIFICATION

Please amend the Specification as follows:

[0040] *Proof Sketch.* Again, membership in NP is trivial if the payoff is PTIME computable. Hardness is shown by embedding the hitting set problem. In this reduction, the attacker plays all exploits and each exploit corresponds with ~~precisely one~~ precisely one vulnerability. This has the effect of imposing a unit cost on each vulnerability. Here, each C_i must be covered by a vulnerability. Hence, the defender must pick a set of all vulnerabilities to meet the cost requirement of DHDP while covering each C_i .

[0050] System Configurations. As noted in FIG. 2, a variety of platforms were represented in our darknet market data. Results are described using application constraints based on common configurations for Windows and Linux servers - as these were the most prominent targets of exploits found on the darknet. In our experiments, software was mapped such as media players, databases, and FTP server software to application constraint sets to model the functional requirements of a system. Experiments were conducted with models for Android, Point-of-Sale, and Apple systems - though qualitatively the results differed little from the Windows and Linux Server experiments.

[0051] DHAP Results. Both the greedy and multiplicative update approaches were implemented to address the DHAP problem. For the greedy algorithm, three variants of greedy (cost-benefit, uniform cost, and combination of the ~~the~~ two) were studied while we varied the parameter ϵ for the multiplicative update approach. Attacker payoff was examined as a function of budget (in Bitcoin). FIGS. 3A and 3B display this result. Though the cost-benefit greedy algorithm has the potential to perform poorly, it was, in general, the best performing approach - despite the multiplicative update approach achieving the better approximation guarantee. Further, the multiplicative update algorithm (Algorithm 2) was consistently the slowest in terms of runtime, taking much longer than the lazy greedy algorithms, particularly for high values of k_{atk} . Despite

the multiplicative update algorithm having a better theoretical approximation ratio when compared to the tandem of greedy algorithms, namely $(1 - \epsilon) (1 - 1/e)$ compared to $\frac{1}{2}(1 - 1/e)$, as shown in FIGS. **3A** and **3B** that the greedy algorithms performed as good as or better than the multiplicative update very consistently. In all algorithms, as expected, runtime grew with budget (not pictured) - though the relationship was not strict, as an increase in budget does not necessarily mean that more exploits will be selected. In the experiments (on a commodity computer equipped with a 3.49 GHz i7 CPU and 16 GB of memory), the runtimes never exceeded ten minutes.

CONCLUSION

Based on the foregoing, Applicants believe that the informalities noted in the Notice of Incomplete Reply have been resolved in compliance with the Notice, and by the present response, Applicant respectfully submits that the application is now in condition for issuance. The Office is invited to telephone Applicants' representative at (602) 650-2000 to facilitate prosecution of this application if there are any further clarifications necessary. If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 50-1662.

Respectfully submitted,

POLSINELLI PC

Date: April 17, 2019

By: /Ari M. Bai/
Ari M. Bai, Reg. No.: 38,726
One E. Washington Street, Suite 1200
Phoenix, AZ 85004
Direct Phone: (602) 650-2000
E-Mail: uspto@polsinelli.com
Attorney for Applicants

UNITED STATES NON-PROVISIONAL PATENT APPLICATION
FOR
SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC
CYBER THREAT MITIGATION

Inventors:

Paulo Shakarian (USA)

John Robertson (USA)

Jana Shakarian (USA)

Vivin Paliath (USA)

Amanda Thart

Priority:

62/261,200 filed on November 30, 2015

Status:

Micro-Entity

Prepared by:

Polsinelli PC

One East Washington Street, Suite 1200

Phoenix, Arizona

Attorney's Docket No.:

055743-555439

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This is a non-provisional application that claims benefit to U.S. provisional application serial number 62/261,200 filed on November 30, 2015, which is herein incorporated by reference in its entirety.

FIELD

[0002] The present disclosure relates to a security game framework, and in particular to a data-driven security game framework that models an attacker based on exploit market data actively mined from the “darknet” or other overlay communication networks to develop strategies for the defender.

BACKGROUND

[0003] Many corporations rely on extensive penetration testing to assess the security of their computer networks. In a penetration test, a red team is hired to expose major flaws in the firm’s security infrastructure. Recently, however, the market for exploit kits has continued to evolve and what was once a rather hard-to-penetrate and exclusive market — whose buyers were primarily western governments -- has now become more accessible to a much wider population. Specifically, the darknet or other overlay network portions of the Internet accessible through anonymization protocols (such as Tor and i2p) have become populated with a variety of markets specializing in such products. In particular, 2015 saw the introduction of darknet markets specializing in zero-day exploit kits — exploits designed to leverage previously undiscovered vulnerabilities. These exploit kits are difficult and time-consuming to develop — and often are sold at premium prices. A survey of 8 marketplaces shows the price ranges of exploit kits for common software in Table 1 — these prices range from 0.0126-8.4 Bit-coin (2.88-1919.06 U.S. dollars at the time of this writing).

[0004] The widespread availability of zero-day exploits in the darknet represents a potential game changer for penetration testers — specifically posing the following questions:

- What exploits will an attacker likely purchase if he targets my organization?
- What software used in the organization pose the biggest risk to new threats?

[0005] Unfortunately, the high cost of a variety of exploits available through the darknet may preclude a penetration tester from obtaining such exploits at a reasonable price to perform an effective penetration testing that accurately accesses the security of a computer network being tested. While criminal activity on the darknet has been extensively studied over the past decade for issues such as drug trade and terrorism, the markets for exploits existing on the darknet are much less well-understood.

Product	Price in BTC	Price in \$*
GovRAT (Source Code + 1 Code Signing Certificate Included)	2.000	\$456.92
Oday Wordpress MU Remote Shell	1.500	\$342.69
A5/I Encryption Rainbow Tables	1.500	\$342.69
Unlimited Code Signing Certificate	1.200	\$274.16
Ready-made Linux botnet 600 SERVERS	1.200	\$274.16
FUD version of Adobe Flash <= 16.0.0.287 (CVE 2015-0311)	1414.68	\$600.00

Product	Price in BTC	Price in \$*
GovRAT (Source Code + 1 Code Signing Certificate Included)	2.000	\$456.92
Oday Wordpress MU Remote Shell	1.500	\$342.69
A5/I Encryption Rainbow Tables	1.500	\$342.69
Unlimited Code Signing Certificate	1.200	\$274.16
Ready-made Linux botnet 600 SERVERS	1.200	\$274.16
FUD version of Adobe Flash <= 16.0.0.287 (CVE 2015-0311)	1414.68	\$600.00

*Price in U.S. Dollar as of Sep. 1, 2015 [1 BTC = \$228.46]

Table 1: Example of Products offered on Darknet Markets

[0006] There has been related work on malicious hacker forums which did not focus on the purchase and sale of specific items. Markets of malicious products relevant to cyber security have been previously studied, but none of these works gathered data on specific exploits (or other products) from either the darkweb or open Internet; nor did they examine the markets through the lens of security games.

[0007] In recent years, “security games” where attacker-defender models are used to inform the actions of defenders in military, law-enforcement, and homeland security applications have gained much traction. With regard to cyber-

security, there have been many contributions including intrusion detection, attack graph based games, and honey-pot placement. However, there does not appear to be a game theoretic approach to host-based defense where the activities of the attacker are informed from an “un-conventional” source (information not directly related to the defender’s system) - specifically information from darknet markets in this case. Further, the very recent emergence of darknet markets specializing in zero-day exploits allow for the integration of information that was previously unknown.

BRIEF DESCRIPTION OF THE DRAWINGS

- [0008] FIG. 1 is a schematic of a real-time exploit analysis system;
- [0009] FIG. 2 is a graph showing the distribution of Exploits with respect to platform;
- [0010] FIG. 3A is a graph showing DHAP Payoff vs. Budget for a Windows server and FIG. 3B is a graph showing the DHAP Payoff vs. Budget for a Linux server;
- [0011] FIG. 4A is a graph showing Defender Best Response, Payoff vs. k_{atk} for Windows server and FIG. 4B is a graph showing Defender Best Response, Payoff vs. k_{atk} for Linux server;
- [0012] FIG. 5 is a simplified block diagram illustrating one embodiment of a game-theoretic framework;
- [0013] FIG. 6 is a simplified block diagram of a computer system; and
- [0014] FIG. 7 is a flowchart of a method for applying a game theoretic cyber threat mitigation to a network.
- [0015] Corresponding reference characters indicate corresponding elements among the view of the drawings. The headings used in the figures do not limit the scope of the claims.

DETAILED DESCRIPTION

[0016] Given a system configuration (or a distribution of system configurations within an organization), the present disclosure models an attacker who, given a budget, will purchase exploits to maximize his level of access to the target system. Likewise, a defender will look to adjust system configurations in an effort to minimize the effectiveness of an attacker while ensuring that necessary software dependencies are satisfied.

[0017] The present system introduces a rigorous and thoroughly analyzed framework for addressing penetration testing that is fed with real-world exploit market data, mined from the darknet. FIG. 1 provides a schematic diagram 100 of our framework. In one embodiment, a new security game framework 100 is designed to model an attacker with access to exploit markets and a defender of information technology infrastructure; theoretical analysis of the framework leading to the development of algorithms to find near-optimal strategies for both players; and an implementation of the system and the results of a thorough suite of experiments on real-world data.

[0018] In some embodiments, the framework 100 includes a security game where the attacker 102 is a malicious hacker with access to a darknet exploit markets 104 and the defender 106 is tasked with host-based defense of either a single or group of systems. The notation V is used herein to represent the entire set of vulnerabilities within a given computer system. Though there may be vulnerabilities not yet detected by the system administrator, information on new vulnerabilities can be mined through an examination of darknet hacking markets. In a real-world organization, system administrators are not able to patch all vulnerabilities for a variety of reasons. Software dependencies, use of legacy systems, and non-availability of patches are some examples. To model this, a “constraint set” (denoted C) is defined as a subset of V . The vulnerabilities in a constraint set represent the vulnerabilities required for some system functionality. When each vulnerability in a constraint set C is in the presented attack surface (i.e. externally accessible), C is then said to be satisfied and the system supports the functionality modeled by C .

[0019] In particular, let C represent the set of all possible constraint sets. This idea is extended with an “application constraint set” which, for an arbitrary

application, i , denoted C_i , is a set of constraint sets (i.e. $C_i \subseteq C$). Each constraint set in C_i represents a set of vulnerabilities that together will provide complete functionality of application i . C_i is said to be satisfied if any single constraint set in C_i is satisfied. If C_i is satisfied by a system configuration, and hence at least one constraint set in C_i is satisfied, application i will properly operate on the system. C is the set of all application constraint sets for a given system configuration and represents all of the applications to be run on the system. So, in this framework, for a given system, a system administrator selects which vulnerabilities may be present in order to allow each application i to function. This begs the question as to how to make this selection. As such, the process is begun by defining some concepts relevant to the adversary.

[0020] The term ex is used to denote a particular exploit - a technique used to take advantage of a given vulnerability. Let Ex denote the set of all possible exploits and Ex denote the set of all possible exploit sets (i.e. $Ex = 2^{Ex}$). For each $ex \in Ex$, c_{ex} is the associated cost of exploit ex - and this is specified directly on a darknet market 104 (normally in Bitcoin). Associated with the set of exploits is the Exploit Function, ExF , which takes a set of exploits as input and returns a set of vulnerabilities (i.e. $ExF : Ex \rightarrow 2^V$). The set of vulnerabilities produced by $ExF(A)$, for a given set of exploits A , represents the vulnerabilities that are exploited by the exploits in A . While many possible variations of an exploit function are possible, in this paper, we will use a straightforward definition that extends the exploit function from singletons (whose associated vulnerabilities can be taken directly from the online marketplaces) to sets of exploits: $ExF(A) = \bigcup_{a \in A} ExF(\{a\})$. For use in proving complexity results, we shall denote the special case where $Ex = V$, $ExF(A) = A$, and $\forall ex \in Ex, c_{ex} = 1$ as the “Identity Exploit Model”.

[0021] Player Strategies and Payoff. An attacker 102 will use a set of exploits to attempt to gain access to a system, and will do so within a budget. Likewise, the defender 106 identifies a set of vulnerabilities that he is willing to expose (often referred to as the “presented attack surface”). Strategies for the two players formally defined as follows.

[0022] Definition 2.1. (Attack Strategy). Given budget $k_{atk} \in \mathbb{R}^+$, an *Attack Strategy*, denoted A is a subset of Ex s.t. $\sum_{a \in A} c_a \leq k_{atk}$.

[0023] Definition 2.2. (Defense Strategy). Given a family of application constraint sets $C = \{C_0, C_1, \dots, C_n\}$, a *Defense Strategy*, denoted D is a subset of V

s.t. for each $C_i \in C$, there exists $C \in C_i$ where $C \subseteq D$.

[0024] Note that when a defense strategy D meets the requirements of C , as per Definition 2.2, we say D *satisfies* C . We will use the notation $\mathbf{A}, \mathbf{D}$ to denote the set of all attack and defense strategies, respectively, and refer to an attacker-defender pair of strategies as a “strategy profile.” We will also define a *mixed strategy* for both players in the normal manner. For the attacker (resp. defender) a mixed strategy is a probability distribution over $\mathbf{A}$ (resp. $\mathbf{D}$). Mixed strategies as Pr_A, Pr_D are normally denoted for each player and use the notation $|Pr_A|$ (resp. $|Pr_D|$) to denote the number of strategies in $\mathbf{A}$ (resp. $\mathbf{D}$) that are assigned a nonzero probability by the mixed strategy. The payoff function may be defined formally as follows:

[0025] Definition 2.3. (Payoff Function). A payoff function, p , is any function that takes a strategy profile as an argument and returns a positive real. Formally, $p : \mathbf{A} \times \mathbf{D} \rightarrow \mathbb{R}^+$

[0026] Unless noted otherwise, the payoff function will be treated as being computable in polynomial time. Also, the payoff function is underspecified - which is designed to allow flexibility in the framework. The following “payoff function axioms” are contemplated:

$$\begin{array}{ll}
 \forall D \in \mathbf{D}, \forall A \in \mathbf{A} \text{ s.t. } \text{Exp}(A) \cap D = \emptyset, p(A, D) = 0 & (1) \\
 \forall D \in \mathbf{D}, \forall D' \subseteq D, \forall A \in \mathbf{A}, p(A, D') \leq p(A, D) & (2) \\
 \forall D \in \mathbf{D}, \forall A \in \mathbf{A}, \forall A' \subseteq A, p(A', D) \leq p(A, D) & (3) \\
 \forall A \in \mathbf{A}, D, D' \in \mathbf{D}, p(A, D) + p(A, D') \geq p(A, D \cup D') & (4) \\
 \forall D \in \mathbf{D}, A, A' \in \mathbf{A}, p(A, D) + p(A', D) \geq p(A \cup A', D) & (5)
 \end{array}$$

$$\begin{array}{ll}
 \forall D \in \mathbf{D}, \forall A \in \mathbf{A} \text{ s.t. } \text{Exp}(A) \cap D = \emptyset, p(A, D) = 0 & (1) \\
 \forall D \in \mathbf{D}, \forall D' \subseteq D, \forall A \in \mathbf{A}, p(A, D') \leq p(A, D) & (2) \\
 \forall D \in \mathbf{D}, \forall A \in \mathbf{A}, \forall A' \subseteq A, p(A', D) \leq p(A, D) & (3) \\
 \forall A \in \mathbf{A}, D, D' \in \mathbf{D}, p(A, D) + p(A, D') \geq p(A, D \cup D') & (4) \\
 \forall D \in \mathbf{D}, A, A' \in \mathbf{A}, p(A, D) + p(A', D) \geq p(A \cup A', D) & (5)
 \end{array}$$

[0027] Axiom 1 states that if the vulnerabilities generated by an attack strategy's exploits and the vulnerabilities in a defense strategy are disjoint sets, the payoff function must return 0. A consequence of axiom 1 is that if either the attack strategy or the defense strategy is the empty set, the payoff function will return 0. Axioms 2 and 3 require the payoff function to be monotonic in the size of the attack and defense strategies. Axioms 4 and 5 require the payoff function to be sub-modular

with respect to the attack and defense strategies.

[0028] The present disclosure focuses on the “over-lap payoff function” which is defined as follows: $p(A,D) = |\text{ExF}(A) \cap D|$. Intuitively, this is simply the number of vulnerabilities exploited by the attacker. Further, when dealing with mixed strategies, payoff in terms of expectation will be discussed. Expected payoff can be formally defined as follows:

$$\text{Exp}(Pr_A, Pr_D) = \sum_{D \in \mathbf{D}} \sum_{A \in \mathbf{A}} Pr_A(A) Pr_D(D) p(A, D)$$

$$\text{Exp}(Pr_A, Pr_D) = \sum_{D \in \mathbf{D}} \sum_{A \in \mathbf{A}} Pr_A(A) Pr_D(D) p(A, D)$$

[0029] Using the overlap function, the expected payoff can be interpreted as the “expected number of exploited vulnerabilities.”

[0030] Best Response Problems. A pair of decision problems dealing with the best response for the players will now be described below. These problems are the deterministic host attacker problem (DHAP) and deterministic host defender problem (DHDP), respectively, and are defined as follows:

DHAP.

[0031] INPUT: $k_{atk} \in \mathbb{R}^+, x \in \mathbb{R}^+, k_{atk} \in \mathbb{R}^+, x \in \mathbb{R}^+$, mixed defense strategy Pr_D , and payoff function p .

[0032] OUTPUT: “Yes” if

$$\exists A \in \mathbf{A} \text{ s.t. } \sum_{a \in A} c_a \leq k_{atk} \text{ and } \sum_{D \in \mathbf{D}} Pr_D(D) p(A, D) \geq x$$

$$\exists A \in \mathbf{A} \text{ s.t. } \sum_{a \in A} c_a \leq k_{atk} \text{ and } \sum_{D \in \mathbf{D}} Pr_D(D) p(A, D) \geq x$$

“No” otherwise.

DHDP.

[0033] INPUT: $x \in \mathbb{R}^+, x \in \mathbb{R}^+$, application constraints C , mixed attack strategy Pr_A , and payoff function p .

[0034] OUTPUT: “Yes” if $\exists D \in \mathbf{D} \text{ s.t. } \sum_{A \in \mathbf{A}} Pr_A(A) p(A, D) \leq x$ and D satisfies C . and “No” otherwise.

[0035] The natural optimization variants for these two problems will deal with maximizing the payoff in DHAP and minimizing the payoff in DHDP.

Analysis and Algorithms

[0036] The complexity and limits of approximation for both DHAP and

DHDP will now be analyzed. The “Identity Exploit Model” is used for the complexity results. Unfortunately, both problems are NP-Complete in the general case.

[0037] Theorem 1. DHAP is NP-Complete, even when $|Pr_D|$ and the payoff function adheres to the submodularity and monotonicity axioms.

[0038] Proof Sketch. Membership in NP is trivial if the payoff is PTIME computable. The hardness result relies on an embedding of the well-known budgeted set cover. Here, the defender’s strategy is treated as a set of elements to cover and the exploits are treated as subsets of D (by virtue of the exploit function). Exploit costs are set as 1 and the attacker’s budget is the value budget from the embedded problem. So, the attacker must pick exploits to meet the budget and cover the determined number of the defender’s vulnerabilities.0

[0039] Theorem 2. When $|C| > 1$ and $|Pr_A| = 1$, DHDP is NP-Complete.

[0040] Proof Sketch. Again, membership in NP is trivial if the payoff is PTIME computable. Hardness is shown by embedding the hitting set problem. In this reduction, the attacker plays all exploits and each exploit corresponds with ~~precisely one~~precisely one vulnerability. This has the effect of imposing a unit cost on each vulnerability. Here, each C_i must be covered by a vulnerability. Hence, the defender must pick a set of all vulnerabilities to meet the cost requirement of DHDP while covering each C_i .

[0041] The hardness of approximation is also analyzed for the optimization variants of DHAP and DHDP. Due to the fact that the above embeddings used set cover and hitting set, we can draw upon the known past results to obtain the following corollaries:

[0042] Corollary 3. DHAP cannot be approximated where the payoff is within a factor of ~~$(1 - \frac{1}{e})$~~ $(1 - \frac{1}{e})$ unless $P = NP$

[0043] Corollary 4. DHDP cannot be approximated where the payoff is within a factor of $(1 - o(1))\ln(n)$ unless $P = NP$

[0044] With the limits of approximation in mind, several algorithms are introduced to solve the optimization variants of DHAP and DHDP. The optimization variant of DHAP under the overlap payoff function is a special case of sub-modular maximization with the distinction that we are not simply picking k discrete objects, but instead picking items that each have a unique cost associated with them. Understanding this, several different approaches are examined to this problem

based on the literature on submodular maximization. DHDP, on the other hand, can be readily approximated using the traditional set-cover algorithm (under some realistic assumptions), as cost does not affect DHDP.

Algorithm 1 Lazy Greedy Algorithm (Cost-Benefit Variant)

Input: $k_{atk} \in \mathbb{R}^+$, Pr_D , and payoff function p .

Output: $A \subseteq Ex$ s.t. $\sum_{a \in A} c_a \leq k_{atk}$

```

1:  $A \leftarrow \emptyset$ ;  $cost \leftarrow 0$ ; priority queue  $Q \leftarrow \emptyset$ ;  $iteration \leftarrow 1$ 
2: for  $e \in Ex$  do
3:    $e.key \leftarrow \frac{\Delta_{Pr_D}(e|\emptyset)}{c_e}$ ;  $e.i \leftarrow 1$ 
4:   insert  $e$  into  $Q$  with “key” as the key
5: end for
6: while  $\{a \in Ex \setminus A : c_a + cost \leq k_{atk}\} \neq \emptyset$  do
7:   extract top (max) element  $e$  of  $Q$ 
8:   if  $e.i = iteration$  then
9:      $A \leftarrow A \cup \{e\}$ ;  $iteration \leftarrow iteration + 1$ 
10:     $cost \leftarrow cost + c_e$ 
11:   else
12:      $e.i \leftarrow iteration$ ;  $e.key \leftarrow \frac{\Delta_{Pr_D}(e|A)}{c_e}$ ;
13:     re-insert  $e$  into  $Q$ 
14:   end if
15: end while
16: return  $A$ 

```

Algorithm 1 Lazy Greedy Algorithm (Cost-Benefit Variant)**Input:** $k_{atk} \in \mathbb{R}^+$, Pr_D , and payoff function p .**Output:** $A \subseteq Ex$ such that $\sum_{a \in A} c_a \leq k_{atk}$

1. $A \leftarrow \emptyset$; $cost \leftarrow 0$; priority queue $Q \leftarrow \emptyset$; $iter \leftarrow 1$
2. **for** $e \in Ex$ **do**
3. $e.key \leftarrow \frac{\Delta_{p, Pr_D}(e | \emptyset)}{c_e}$; $e.i \leftarrow 1$
4. Insert e into Q with $e.key$ as its key
5. **end for**
6. **while** $\{a \in Ex \setminus A : c_a + cost \leq k_{atk}\} \neq \emptyset$ **do**
7. extract top (max) element e of Q
8. **if** $e.i = iter$ and $c_e + cost \leq k_{atk}$ **then**
9. $A \leftarrow A \cup \{e\}$; $iter \leftarrow iter + 1$
10. $cost \leftarrow cost + c_e$
11. **else if** $c_e + cost \leq k_{atk}$ **then**
12. $e.i \leftarrow iter$; $e.key \leftarrow \frac{\Delta_{p, Pr_D}(e | A)}{c_e}$
13. re-insert e into Q
14. **end if**
15. **end while**
16. **return** A

Algorithms for DHAP

[0045] Greedy Approaches. As mentioned earlier, the non-unit cost of exploits mean that DHAP can be considered as a submodular maximization problem subject to knapsack constraints. Two versions of the traditional greedy algorithm can be applied: a cost-benefit variant and uniform-cost variant, both of which will also use the lazy-greedy optimization to further enhance performance while maintaining the approximation guarantee. It was independently noted that the uniform-cost and the cost-benefit algorithms can perform arbitrarily badly. However, by extending a result from either the cost-benefit or the uniform-cost algorithm will provide a solution within a factor of $\frac{1}{2}(1 - 1/e)$ for a given set of input parameters. By applying both algorithms to a given problem instance and returning the attack strategy which produces the larger payoff, the $\frac{1}{2}(1 - 1/e)$ approximation factor is achieved for DHAP. A cost-benefit lazy approximation algorithm is shown in Algorithm 1. By removing “ c_e ” from the denominator in the $e.key$ assignment in lines 3 and 12, the cost benefit lazy

approximation algorithm is transformed into a uniform cost lazy approximation algorithm.

[0046] Multiplicative Update Approach. An improved approximation ratio, when compared with the $\frac{1}{2}(1 - 1/e)$ ratio for the greedy algorithms, can be obtained by adapting Algorithm 1 for DHAP. This is shown as Algorithm 2 in this disclosure. For some value ϵ (a parameter), this algorithm provides a $(1 - \epsilon)(1 - 1/e)$ approximation of the optimal solution (Theorem 1.2), which, by providing an exceedingly small ϵ value, can get arbitrarily close to the $\frac{1}{2}(1 - 1/e)$ optimal approximation limit we discussed earlier.

Algorithm 2 Multiplicative Update

Input: $k_{atk}, \epsilon \in \mathbb{R}^+$ s.t. $0 < \epsilon \leq 1$, Pr_D , and payoff function p .

Output: $A \subseteq E$ s.t. $\sum_{u \in A} c_u \leq k_{atk}$.

```

1:  $E_{x'} \leftarrow \{ex \in E : c_{ex} \leq k_{atk}\}$ 
2:  $A \leftarrow \emptyset$ 
3:  $W \leftarrow \min_{ex' \in E_{x'}} k_{atk}^2 / c_{ex'}$ 
4:  $w \leftarrow 1/k_{atk}$ ;  $\lambda \leftarrow e^{W/4}$ 
5: while  $k_{atk}w \leq \lambda$  and  $E_{x'} \neq \emptyset$  do
6:    $ex_j \leftarrow \operatorname{argmin}_{ex_j \in E_{x'} \setminus A} \frac{c_{ex_j}}{k_{atk}} w / \Delta_{p, Pr_D}(ex_j | A)$ 
7:    $A \leftarrow A \cup \{ex_j\}$ 
8:    $w \leftarrow w \lambda^{c_{ex_j} / k_{atk}^2}$ 
9:    $E_{x'} \leftarrow E_{x'} \setminus \{ex_j\}$ 
10: end while
11: if  $\sum_{D \in Pr_D} Pr_D(D) p(A, D) \leq k_{atk}$  then
12:   return  $A$ 
13: else if  $\sum_{D \in Pr_D} Pr_D(D) p(A \setminus \{ex_j\}, D) \geq \sum_{D \in Pr_D} Pr_D(D) p(\{ex_j\}, D)$  then
14:   return  $A \setminus \{ex_j\}$ 
15: else
16:   return  $\{ex_j\}$ 
17: end if
```

Algorithm 2 Multiplicative Update

Input: $k_{atk}, \epsilon \in \mathbb{R}^+$ such that $0 < \epsilon < 1$, Pr_D , and payoff function p .

Output: $A \subseteq Ex$ s.t. $\sum_{a \in A} c_a \leq k_{atk}$

1. $Ex' \leftarrow \{ex \in Ex : c_{ex} \leq k_{atk}\}$
 2. $A \leftarrow \emptyset$
 3. $W \leftarrow \min_{ex'_i \in [Ex'] } k_{atk}^2 / c_{ex'_i}$
 4. $w \leftarrow \frac{1}{k_{atk}}; \lambda \leftarrow e^{\frac{\epsilon W}{4}}$
 5. **while** $k_{atk}w \leq \lambda$ and $Ex' \neq \emptyset$ **do**
 6. $ex_j \leftarrow \operatorname{argmin}_{ex_j \in Ex' \setminus A} (\frac{c_{ex_j}}{k_{atk}} w / \Delta_{p, Pr_D}(ex_j | A))$
 7. $A \leftarrow A \cup \{ex_j\}$
 8. $w \leftarrow w \lambda^{c_{ex_j} / k_{atk}^2}$
 9. $Ex' \leftarrow Ex' \setminus \{ex_j\}$
 10. **end while**
 11. **if** $\sum_{A_i \in A} c_{A_i} \leq k_{atk}$ **then**
 12. **return** A
 13. **else if** $\sum_{D \in Pr_D} Pr_D(D) p(A \setminus \{ex_j\}, D) \geq \sum_{D \in Pr_D} Pr_D(D) p(\{ex_j\}, D)$ **then**
 14. **return** $A \setminus \{ex_j\}$
 15. **else**
 16. **return** $\{ex_j\}$
 17. **end if**
-

[0047] Algorithm for DHDP. When using the overlap payoff function,

DHDP can be modeled as a weighted set cover problem. Because the overlap payoff function is a modular function, the associated cost of a given vulnerability v , is simply the payoff produced by the singleton set $\{v\}$ with a mixed attack strategy. In the common case where each constraint set is a singleton set, if the overlap payoff function is used, an adaptation on the standard greedy weighted set cover algorithm can be used for DHDP (Algorithm 3), providing a $\ln(n) + 1$ approximation,

Evaluation and Discussion

[0048] **Darknet Market Data.** Eight marketplaces located on the Tor

network were scraped and parsed during the month of May 2015. Each of these markets host vendors offering “hacking tools”, including malware, botnets, exploits and other means serving to breach, steal and otherwise manipulate virtual targets. The product list is comprised of 235 such hacking tools, 167 of which were distinct.

Algorithm 3 Weighted Greedy DHDP Algorithm for Singleton Constraint Set and Overlap Payoff Function Case

Input: Vulnerabilities V , Pr_A , and application constraints $\mathcal{C}$.

Output: $D \subseteq V$ s.t. the application constraints $\mathcal{C}$ are satisfied.

```

1:  $D \leftarrow \emptyset$ 
2:  $S \leftarrow$  set s.t.  $S_i = \{j : V_i \in C_j \text{ where } V_i \text{ is } i\text{th vulnerability in } V\}$ 
3:  $c_{S_i} \leftarrow \sum_{A \in Pr_A} Pr_A(A) |ExF(A) \cap \{V_i\}|$ 
4:  $\mathcal{C}' \leftarrow [\mathcal{C}]$ 
5: while  $\mathcal{C}' \neq \emptyset$  do
6:    $S_i \leftarrow \operatorname{argmax}_{S_i \in S} \frac{|S_i \cap \mathcal{C}'|}{c_{S_i}}$ 
7:    $\mathcal{C}' \leftarrow \mathcal{C}' \setminus S_i$ 
8:    $D \leftarrow D \cup \{V_i\}$ 
9: end while
10: return  $D$ 

```

Algorithm 3 Weighted Greedy DHDP Algorithm for Singleton Constraint Set and Overlap Payoff Case

Input: Vulnerabilities V , Pr_A , and application constraints $\mathcal{C}$

Output: $D \subseteq V$ s.t. the application constraints $\mathcal{C}$ are satisfied

```

1.  $D \leftarrow \emptyset$ 
2.  $S \leftarrow$  set such that  $S_i = \{j : V_i \in C_j \text{ where } V_i \text{ is the } i\text{th vulnerability in } V\}$ 
3.  $c_{S_i} \leftarrow \sum_{A \in Pr_A} Pr_A(A) |ExF(A) \cap \{V_i\}|$ 
4.  $\mathcal{C}' \leftarrow [\mathcal{C}]$ 
5. while  $\mathcal{C}' \neq \emptyset$  do
6.    $S_i \leftarrow \operatorname{argmax}_{S_i \in S} \frac{|S_i \cap \mathcal{C}'|}{c_{S_i}}$ 
7.    $\mathcal{C}' \leftarrow \mathcal{C}' \setminus S_i$ 
8.    $D \leftarrow D \cup \{V_i\}$ 
9. end while
10. return  $D$ 

```

[0049] It found several identical products being sold on more than one market usually by the same seller (using an identical online handle). The products targeted 21 specific platforms, such as different versions of Adobe Flash, Linux, MSWindows and OS X as well as online presences such as Facebook, Wordpress and others. Hardware-related software such as those associated with Point-of-Sale machines, routers, and servers are also reflected in this number. FIG. 2 illustrates the variety of products in the markets and Table 2 illustrates exemplar exploits.

[0050] System Configurations. As noted in FIG. 2, a variety of platforms were represented in our darknet market data. Results are described using application constraints based on common configurations for Windows and Linux

servers - as these were the most prominent targets of exploits found on the darknet. In our experiments, software was mapped such as media players, databases, and FTP server software to application constraint sets to model the functional requirements of a system. Experiments were conducted with models for Android, Point-of-Sale, and Apple systems - though qualitatively the results differed little from the Windows and Linux Server experiments.

[0051] DHAP Results. Both the greedy and multiplicative update approaches were implemented to address the DHAP problem. For the greedy algorithm, three variants of greedy (cost-benefit, uniform cost, and combination of the ~~the~~ two) were studied while we varied the parameter ϵ for the multiplicative update approach. Attacker payoff was examined as a function of budget (in Bitcoin). FIGS. **3A** and **3B** display this result. Though the cost-benefit greedy algorithm has the potential to perform poorly, it was, in general, the best performing approach - despite the multiplicative update approach achieving the better approximation guarantee. Further, the multiplicative update algorithm (Algorithm 2) was consistently the slowest in terms of runtime, taking much longer than the lazy greedy algorithms, particularly for high values of k_{atk} . Despite the multiplicative update algorithm having a better theoretical approximation ratio when compared to the tandem of greedy algorithms, namely $(1 - \epsilon) (1 - 1/e)$ compared to $\frac{1}{2}(1 - 1/e)$, as shown in FIGS. **3A** and **3B** that the greedy algorithms performed as good as or better than the multiplicative update very consistently. In all algorithms, as expected, runtime grew with budget (not pictured) - though the relationship was not strict, as an increase in budget does not necessarily mean that more exploits will be selected. In the experiments (on a commodity computer equipped with a 3.49 GHz i7 CPU and 16 GB of memory), the runtimes never exceeded ten minutes.

[0052] DHDP Results. FIGS. **4A** and **4B** demonstrate a defender's best response to an attack strategy against a Windows Server and Linux Server, respectively, for varying values of k_{atk} . Though similar trends are shown in FIGS. **3A** and **3B** as are shown in FIGS. **4A** and **4B**, the payoff is generally lower, meaning that the defender can lower the expected payoff by enacting a best response strategy to an attack strategy produced by DHAP - which in the framework translates to fewer exploited vulnerabilities.

[0053] Exploit Payoff Analysis. Instead of altering the software that appears on the host system in an attempt to avoid exploits, such as in the best

response approach, in exploit payoff analysis, the defender will identify which specific exploits are increasing the payoff the most, with a hope that the defender can reverse-engineer the exploit, or patch the vulnerability himself. To identify which exploits should be reverse-engineered, the defender first runs DHAP against his host system to identify what payoff an attacker could expect to produce. Then, for each exploit ex , the defender runs DHAP against the host with the set of exploits $Ex \setminus \{ex\}$. The exploit ex that, when removed from the universe of exploits Ex , produces the largest drop in payoff for the attacker is the exploit that the defender should attempt to reverse-engineer. More formally, let A be the attack strategy produced by DHAP when using Ex as the universe of exploits and let A_{ex} be the attack strategy that is produced when DHAP is run against the host when using $Ex \setminus \{ex\}$ as the universe of exploits. The defender will attempt to reverse-engineer the exploit, where D is the defense strategy representing the host. To account for exploits that, though they greatly reduce payoff when removed from Ex , may be too expensive for the defender to purchase, a cost-benefit analysis is also considered where the decrease in payoff is normalized by the cost of the exploit. The top exploits to reverse-engineer to defend a Windows Server host when considering an attacker budget of $k_{atk} = 5$, are shown in Table 3 with columns for both maximum payoff reduction and maximum cost-benefit analysis.

Prod.	Vuln.	Target	USD
Kernel Panic	X-display system	Linux <= 3.13.0-43	\$471.56
IE <= 11	memory corr.	IE on Windows <= 7	\$35.00
RemoteShell	wpconfig.php	Wordpress MU	\$1,500.00
oday RCE	WebView memory corr.	Android 4.1, 4.2	\$36.50
WindowsLPE	win32k elev. of priv.	Windows <= 8.1	\$12.00-48.17
MS15-034 RCE	http.sys	Windows <= 8.1	\$311.97
FUD Flash Exp.	unspec.	FlashPlayer <= 16.0.0.287	\$600.00

Prod.	Vuln.	Target	USD
Kernel Panic	X-display system	Linux <= 3.13.0-48	\$471.56
IE <= 11	memory corr.	IE on Windows <= 7	\$35.00
RemoteShell	wpconfig.php	Wordpress MU	\$1,500.00
oday RCE	WebView memory corr.	Android 4.1, 4.2	\$36.50
WindowsLPE	Win32k elev. of priv.	Windows <= 8.1	\$12.00-48.17
MS15-034 RCE	http.sys	Windows <= 8.1	\$311.97
FUD Flash Exp.	unspec.	FlashPlayer <= 16.0.0.287	\$600.00

Table 2: Examples of Exploits from Darknet Markets

Exploit	Max. Payoff Reduction	Max. Cost-Benefit	Exploit Cost (BTC)
SMTP Mail Cracker	1	4.757	0.2102
SUPEE-5433	1	1.190	0.8404
Hack ICQ	1	79.089	0.01264
Plasma	0.6677	1.582	0.2563
Wordpress Exploiter	0.6677	2.6467	0.2102
CVE-2014-0160	0.6677	3.178	0.2101

Exploit	Max. Payoff Reduction	Max. Cost-Benefit	Exploit Cost (BTC)
SMTP Mail Cracker	1	4.757	0.2102
SUPEE-5433	1	1.190	0.8404
Hack ICQ	1	79.089	0.01264
Plasma	0.6677	1.582	0.2563
Wordpress Exploiter	0.6677	2.6467	0.2102
CVE-2014-0160	0.6677	3.178	0.2101

Table 3: Defender Exploit Analysis for $k_{atk} = 5$ Game Theoretic Framework

In some embodiments, to leverage the data collected from the darknet, a game theoretic framework is disclosed to reason about a defender facing an attacker sourced through the communities on the darknet. The paradigm used for this is based on the framework of a “security game”. Such a framework 500 is designed from the ground-up to consider marketplace information a simplified block diagram is shown in FIG. 5. In this framework, an attacker has a strategy (denoted A) that consists of a set of exploits he must purchase within a given budget. An exploit function (denoted Ex) maps the attacker's strategy to a set of vulnerable software applications, which can be easily obtained from darknet marketplace data. Meanwhile, the set of applications on a defender's system D is treated as his strategy. While the payoff function is defined in terms of axioms, a simple payoff function can be the cardinality of the overlap -- $p(A, D) = |Ex(A) \cap D|$. The NP-hard problems of finding optimal strategies for both players and developed approximation algorithms are disclosed. A mixed strategy of attack and defense is disclosed that provides a natural extension for populations of computer systems as opposed to a single host as well as the modeling of multiple attackers.

[0054] Referring to FIG. 6, a detailed description of an example computing system 600 having one or more computing units that may implement various systems and methods discussed herein is provided. The computing system 600 may be applicable to the system described herein. For example, the computing system 600 may form a portion of the theoretical game engine 504 of FIG. 5

discussed above. It will be appreciated that specific implementations of these devices may be of differing possible specific computing architectures not all of which are specifically discussed herein but will be understood by those of ordinary skill in the art.

[0055] The computer system 600 may be a computing system is capable of executing a computer program product to execute a computer process. Data and program files may be input to the computer system 600, which reads the files and executes the programs therein. Some of the elements of the computer system 600 are shown in FIG. 6, including one or more hardware processors 602, one or more data storage devices 604, one or more memory devices 606, and/or one or more ports 608-612. Additionally, other elements that will be recognized by those skilled in the art may be included in the computing system 600 but are not explicitly depicted in Fig. 6 or discussed further herein. Various elements of the computer system 600 may communicate with one another by way of one or more communication buses, point-to-point communication paths, or other communication means not explicitly depicted in FIG. 6.

[0056] The processor 602 may include, for example, a central processing unit (CPU), a microprocessor, a microcontroller, a digital signal processor (DSP), and/or one or more internal levels of cache. There may be one or more processors 602, such that the processor comprises a single central-processing unit, or a plurality of processing units capable of executing instructions and performing operations in parallel with each other, commonly referred to as a parallel processing environment.

[0057] The computer system 600 may be a conventional computer, a distributed computer, or any other type of computer, such as one or more external computers made available via a cloud computing architecture. The presently described technology is optionally implemented in software stored on the data stored device(s) 604, stored on the memory device(s) 606, and/or communicated via one or more of the ports 608-612, thereby transforming the computer system 600 in FIG. 6 to a special purpose machine for implementing the operations described herein. Examples of the computer system 600 include personal computers, terminals, workstations, mobile phones, tablets, laptops, personal computers, multimedia consoles, gaming consoles, set top boxes, and the like.

[0058] The one or more data storage devices 604 may include any non-volatile data storage device capable of storing data generated or employed within the computing system 600, such as computer executable instructions for performing a computer process, which may include instructions of both application programs and an operating system (OS) that manages the various components of the computing system 600. The data storage devices 604 may include, without limitation, magnetic disk drives, optical disk drives, solid state drives (SSDs), flash drives, and the like. The data storage devices 604 may include removable data storage media, non-removable data storage media, and/or external storage devices made available via a wired or wireless network architecture with such computer program products, including one or more database management products, web server products, application server products, and/or other additional software components. Examples of removable data storage media include Compact Disc Read-Only Memory (CD-ROM), Digital Versatile Disc Read-Only Memory (DVD-ROM), magneto-optical disks, flash drives, and the like. Examples of non-removable data storage media include internal magnetic hard disks, SSDs, and the like. The one or more memory devices 606 may include volatile memory (e.g., dynamic random access memory (DRAM), static random access memory (SRAM), etc.) and/or non-volatile memory (e.g., read-only memory (ROM), flash memory, etc.).

[0059] Computer program products containing mechanisms to effectuate the systems and methods in accordance with the presently described technology may reside in the data storage devices 604 and/or the memory devices 606, which may be referred to as machine-readable media. It will be appreciated that machine-readable media may include any tangible non-transitory medium that is capable of storing or encoding instructions to perform any one or more of the operations of the present disclosure for execution by a machine or that is capable of storing or encoding data structures and/or modules utilized by or associated with such instructions. Machine-readable media may include a single medium or multiple media (e.g., a centralized or distributed database, and/or associated caches and servers) that store the one or more executable instructions or data structures.

[0060] In some implementations, the computer system 600 includes one or more ports, such as an input/output (I/O) port 608, a communication port 610, and a sub-systems port 612, for communicating with other computing, network, or

vehicle devices. It will be appreciated that the ports 608-612 may be combined or separate and that more or fewer ports may be included in the computer system 600.

[0061] The I/O port 608 may be connected to an I/O device, or other device, by which information is input to or output from the computing system 600. Such I/O devices may include, without limitation, one or more input devices, output devices, and/or environment transducer devices.

[0062] In one implementation, the input devices convert a human-generated signal, such as, human voice, physical movement, physical touch or pressure, and/or the like, into electrical signals as input data into the computing system 600 via the I/O port 608. Similarly, the output devices may convert electrical signals received from computing system 600 via the I/O port 608 into signals that may be sensed as output by a human, such as sound, light, and/or touch. The input device may be an alphanumeric input device, including alphanumeric and other keys for communicating information and/or command selections to the processor 602 via the I/O port 608. The input device may be another type of user input device including, but not limited to: direction and selection control devices, such as a mouse, a trackball, cursor direction keys, a joystick, and/or a wheel; one or more sensors, such as a camera, a microphone, a positional sensor, an orientation sensor, a gravitational sensor, an inertial sensor, and/or an accelerometer; and/or a touch-sensitive display screen ("touchscreen"). The output devices may include, without limitation, a display, a touchscreen, a speaker, a tactile and/or haptic output device, and/or the like. In some implementations, the input device and the output device may be the same device, for example, in the case of a touchscreen.

[0063] In one implementation, a communication port 610 is connected to a network by way of which the computer system 600 may receive network data useful in executing the methods and systems set out herein as well as transmitting information and network configuration changes determined thereby. Stated differently, the communication port 610 connects the computer system 600 to one or more communication interface devices configured to transmit and/or receive information between the computing system 600 and other devices by way of one or more wired or wireless communication networks or connections. For example, the computer system 600 may be instructed to access information stored in a public network, such as the Internet. The computer 600 may then utilize the communication port to access one or more publicly available servers that store

information in the public network. In one particular embodiment, the computer system 600 uses an Internet browser program to access a publicly available website. The website is hosted on one or more storage servers accessible through the public network. Once accessed, data stored on the one or more storage servers may be obtained or retrieved and stored in the memory device(s) 606 of the computer system 600 for use by the various modules and units of the system, as described herein.

[0064] Examples of types of networks or connections of the computer system 600 include, without limitation, Universal Serial Bus (USB), Ethernet, Wi-Fi, Bluetooth®, Near Field Communication (NFC), Long-Term Evolution (LTE), and so on. One or more such communication interface devices may be utilized via the communication port 610 to communicate one or more other machines, either directly over a point-to-point communication path, over a wide area network (WAN) (e.g., the Internet), over a local area network (LAN), over a cellular (e.g., third generation (3G) or fourth generation (4G)) network, or over another communication means. Further, the communication port 610 may communicate with an antenna for electromagnetic signal transmission and/or reception.

[0065] The computer system 600 may include a sub-systems port 612 for communicating with one or more additional systems to perform the operations described herein. For example, the computer system 600 may communicate through the sub-systems port 612 with a large processing system to perform one or more of the calculations discussed above.

[0066] The system set forth in FIG. 6 is but one possible example of a computer system that may employ or be configured in accordance with aspects of the present disclosure. It will be appreciated that other non-transitory tangible computer-readable storage media storing computer-executable instructions for implementing the presently disclosed technology on a computing system may be utilized.

[0067] FIG. 7 is a flowchart of a method for applying game theoretic cyber threat mitigation to a network. In one particular embodiment, the operations of the method 700 may be executed by the computing device described above in relation to FIG. 6. Thus, the computing device may utilize a network connection to a public network to obtain a set of exploits to attack a device or network, such as in operation 702. In some instances, the set of exploits may be obtained from the

UNITED STATES NON-PROVISIONAL PATENT APPLICATION
FOR
SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC
CYBER THREAT MITIGATION

Inventors:

Paulo Shakarian (USA)

John Robertson (USA)

Jana Shakarian (USA)

Vivin Paliath (USA)

Amanda Thart

Priority:

62/261,200 filed on November 30, 2015

Status:

Micro-Entity

Prepared by:

Polsinelli PC
One East Washington Street, Suite 1200
Phoenix, Arizona

Attorney's Docket No.:

055743-555439

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This is a non-provisional application that claims benefit to U.S. provisional application serial number 62/261,200 filed on November 30, 2015, which is herein incorporated by reference in its entirety.

FIELD

[0002] The present disclosure relates to a security game framework, and in particular to a data-driven security game framework that models an attacker based on exploit market data actively mined from the “darknet” or other overlay communication networks to develop strategies for the defender.

BACKGROUND

[0003] Many corporations rely on extensive penetration testing to assess the security of their computer networks. In a penetration test, a red team is hired to expose major flaws in the firm’s security infrastructure. Recently, however, the market for exploit kits has continued to evolve and what was once a rather hard-to-penetrate and exclusive market — whose buyers were primarily western governments -- has now become more accessible to a much wider population. Specifically, the darknet or other overlay network portions of the Internet accessible through anonymization protocols (such as Tor and i2p) have become populated with a variety of markets specializing in such products. In particular, 2015 saw the introduction of darknet markets specializing in zero-day exploit kits — exploits designed to leverage previously undiscovered vulnerabilities. These exploit kits are difficult and time-consuming to develop — and often are sold at premium prices. A survey of 8 marketplaces shows the price ranges of exploit kits for common software in Table 1 — these prices range from 0.0126-8.4 Bit-coin (2.88-1919.06 U.S. dollars at the time of this writing).

[0004] The widespread availability of zero-day exploits in the darknet represents a potential game changer for penetration testers — specifically posing the following questions:

- What exploits will an attacker likely purchase if he targets my organization?
- What software used in the organization pose the biggest risk to new threats?

[0005] Unfortunately, the high cost of a variety of exploits available through the darknet may preclude a penetration tester from obtaining such exploits at a reasonable price to perform an effective penetration testing that accurately accesses the security of a computer network being tested. While criminal activity on the darknet has been extensively studied over the past decade for issues such as drug trade and terrorism, the markets for exploits existing on the darknet are much less well-understood.

Product	Price in BTC	Price in \$*
GovRAT (Source Code + 1 Code Signing Certificate Included)	2,000	\$456.92
Oday Wordpress MU Remote Shell	1,500	\$342.69
A5/I Encryption Rainbow Tables	1,500	\$342.69
Unlimited Code Signing Certificate	1,200	\$274.16
Ready-made Linux botnet 600 SERVERS	1,200	\$274.16
FUD version of Adobe Flash <= 16.0.0.287 (CVE 2015-0311)	1414.68	\$600.00

*Price in U.S. Dollar as of Sep. 1, 2015 [1 BTC = \$228.46]

Table 1: Example of Products offered on Darknet Markets

[0006] There has been related work on malicious hacker forums which did not focus on the purchase and sale of specific items. Markets of malicious products relevant to cyber security have been previously studied, but none of these works gathered data on specific exploits (or other products) from either the darkweb or open Internet; nor did they examine the markets through the lens of security games.

[0007] In recent years, “security games” where attacker-defender models are used to inform the actions of defenders in military, law-enforcement, and homeland security applications have gained much traction. With regard to cyber-security, there have been many contributions including intrusion detection, attack graph based games, and honey-pot placement. However, there does not appear to be a game theoretic approach to host-based defense where the activities of the attacker are informed from an “un-conventional” source (information not directly related to the defender’s system) - specifically information from darknet markets in this case. Further, the very recent emergence of darknet markets specializing in zero-day exploits allow for the integration of information that was previously

unknown.

BRIEF DESCRIPTION OF THE DRAWINGS

- [0008] FIG. 1 is a schematic of a real-time exploit analysis system;
- [0009] FIG. 2 is a graph showing the distribution of Exploits with respect to platform;
- [0010] FIG. 3A is a graph showing DHAP Payoff vs. Budget for a Windows server and FIG. 3B is a graph showing the DHAP Payoff vs. Budget for a Linux server;
- [0011] FIG. 4A is a graph showing Defender Best Response, Payoff vs. k_{atk} for Windows server and FIG. 4B is a graph showing Defender Best Response, Payoff vs. k_{atk} for Linux server;
- [0012] FIG. 5 is a simplified block diagram illustrating one embodiment of a game-theoretic framework;
- [0013] FIG. 6 is a simplified block diagram of a computer system; and
- [0014] FIG. 7 is a flowchart of a method for applying a game theoretic cyber threat mitigation to a network.
- [0015] Corresponding reference characters indicate corresponding elements among the view of the drawings. The headings used in the figures do not limit the scope of the claims.

DETAILED DESCRIPTION

[0016] Given a system configuration (or a distribution of system configurations within an organization), the present disclosure models an attacker who, given a budget, will purchase exploits to maximize his level of access to the target system. Likewise, a defender will look to adjust system configurations in an effort to minimize the effectiveness of an attacker while ensuring that necessary software dependencies are satisfied.

[0017] The present system introduces a rigorous and thoroughly analyzed framework for addressing penetration testing that is fed with real-world exploit market data, mined from the darknet. FIG. 1 provides a schematic diagram 100 of our framework. In one embodiment, a new security game framework 100 is designed to model an attacker with access to exploit markets and a defender of information technology infrastructure; theoretical analysis of the framework leading to the development of algorithms to find near-optimal strategies for both players; and an implementation of the system and the results of a thorough suite of experiments on real-world data.

[0018] In some embodiments, the framework 100 includes a security game where the attacker 102 is a malicious hacker with access to a darknet exploit markets 104 and the defender 106 is tasked with host-based defense of either a single or group of systems. The notation V is used herein to represent the entire set of vulnerabilities within a given computer system. Though there may be vulnerabilities not yet detected by the system administrator, information on new vulnerabilities can be mined through an examination of darknet hacking markets. In a real-world organization, system administrators are not able to patch all vulnerabilities for a variety of reasons. Software dependencies, use of legacy systems, and non-availability of patches are some examples. To model this, a “constraint set” (denoted C) is defined as a subset of V . The vulnerabilities in a constraint set represent the vulnerabilities required for some system functionality. When each vulnerability in a constraint set C is in the presented attack surface (i.e. externally accessible), C is then said to be satisfied and the system supports the functionality modeled by C .

[0019] In particular, let C represent the set of all possible constraint sets. This idea is extended with an “application constraint set” which, for an arbitrary

application, i , denoted C_i , is a set of constraint sets (i.e. $C_i \subseteq C$). Each constraint set in C_i represents a set of vulnerabilities that together will provide complete functionality of application i . C_i is said to be satisfied if any single constraint set in C_i is satisfied. If C_i is satisfied by a system configuration, and hence at least one constraint set in C_i is satisfied, application i will properly operate on the system. C is the set of all application constraint sets for a given system configuration and represents all of the applications to be run on the system. So, in this framework, for a given system, a system administrator selects which vulnerabilities may be present in order to allow each application i to function. This begs the question as to how to make this selection. As such, the process is begun by defining some concepts relevant to the adversary.

[0020] The term ex is used to denote a particular exploit - a technique used to take advantage of a given vulnerability. Let Ex denote the set of all possible exploits and Ex denote the set of all possible exploit sets (i.e. $Ex = 2^{Ex}$). For each $ex \in Ex$, c_{ex} is the associated cost of exploit ex - and this is specified directly on a darknet market 104 (normally in Bitcoin). Associated with the set of exploits is the Exploit Function, ExF , which takes a set of exploits as input and returns a set of vulnerabilities (i.e. $ExF : Ex \rightarrow 2^V$). The set of vulnerabilities produced by $ExF(A)$, for a given set of exploits A , represents the vulnerabilities that are exploited by the exploits in A . While many possible variations of an exploit function are possible, in this paper, we will use a straightforward definition that extends the exploit function from singletons (whose associated vulnerabilities can be taken directly from the online marketplaces) to sets of exploits: $ExF(A) = \bigcup_{a \in A} ExF(\{a\})$. For use in proving complexity results, we shall denote the special case where $Ex = V$, $ExF(A) = A$, and $\forall ex \in Ex, c_{ex} = 1$ as the “Identity Exploit Model”.

[0021] Player Strategies and Payoff. An attacker 102 will use a set of exploits to attempt to gain access to a system, and will do so within a budget. Likewise, the defender 106 identifies a set of vulnerabilities that he is willing to expose (often referred to as the “presented attack surface”). Strategies for the two players formally defined as follows.

[0022] Definition 2.1. (Attack Strategy). Given budget $k_{atk} \in \mathbb{R}^+$, an *Attack Strategy*, denoted A is a subset of Ex s.t. $\sum_{a \in A} c_a \leq k_{atk}$.

[0023] Definition 2.2. (Defense Strategy). Given a family of application constraint sets $C = \{C_0, C_1, \dots, C_n\}$, a *Defense Strategy*, denoted D is a subset of V

s.t. for each $C_i \in C$, there exists $C \in C_i$ where $C \subseteq D$.

[0024] Note that when a defense strategy D meets the requirements of C , as per Definition 2.2, we say D *satisfies* C . We will use the notation $\mathbf{A}$, $\mathbf{D}$ to denote the set of all attack and defense strategies, respectively, and refer to an attacker-defender pair of strategies as a “strategy profile.” We will also define a *mixed strategy* for both players in the normal manner. For the attacker (resp. defender) a mixed strategy is a probability distribution over $\mathbf{A}$ (resp. $\mathbf{D}$). Mixed strategies as Pr_A , Pr_D are normally denoted for each player and use the notation $|Pr_A|$ (resp. $|Pr_D|$) to denote the number of strategies in $\mathbf{A}$ (resp. $\mathbf{D}$) that are assigned a nonzero probability by the mixed strategy. The payoff function may be defined formally as follows:

[0025] Definition 2.3. (Payoff Function). A payoff function, p , is any function that takes a strategy profile as an argument and returns a positive real. Formally, $p : \mathbf{A} \times \mathbf{D} \rightarrow \mathbb{R}^+$

[0026] Unless noted otherwise, the payoff function will be treated as being computable in polynomial time. Also, the payoff function is underspecified - which is designed to allow flexibility in the framework. The following “payoff function axioms” are contemplated:

$$\forall D \in \mathbf{D}, \forall A \in \mathbf{A} \text{ s.t. } \text{ExF}(A) \cap D = \emptyset, p(A, D) = 0 \quad (1)$$

$$\forall D \in \mathbf{D}, \forall D' \subseteq D, \forall A \in \mathbf{A}, p(A, D') \leq p(A, D) \quad (2)$$

$$\forall D \in \mathbf{D}, \forall A \in \mathbf{A}, \forall A' \subseteq A, p(A', D) \leq p(A, D) \quad (3)$$

$$\forall A \in \mathbf{A}, D, D' \in \mathbf{D}, p(A, D) + p(A, D') \geq p(A, D \cup D') \quad (4)$$

$$\forall D \in \mathbf{D}, A, A' \in \mathbf{A}, p(A, D) + p(A', D) \geq p(A \cup A', D) \quad (5)$$

[0027] Axiom 1 states that if the vulnerabilities generated by an attack strategy's exploits and the vulnerabilities in a defense strategy are disjoint sets, the payoff function must return 0. A consequence of axiom 1 is that if either the attack strategy or the defense strategy is the empty set, the payoff function will return 0. Axioms 2 and 3 require the payoff function to be monotonic in the size of the attack and defense strategies. Axioms 4 and 5 require the payoff function to be sub-modular with respect to the attack and defense strategies.

[0028] The present disclosure focuses on the “over-lap payoff function” which is defined as follows: $p(A, D) = |\text{ExF}(A) \cap D|$. Intuitively, this is simply the number of vulnerabilities exploited by the attacker. Further, when dealing with mixed

strategies, payoff in terms of expectation will be discussed. Expected payoff can be formally defined as follows:

$$Exp(Pr_A, Pr_D) = \sum_{D \in \mathbf{D}} \sum_{A \in \mathbf{A}} Pr_A(A) Pr_D(D) p(A, D)$$

[0029] Using the overlap function, the expected payoff can be interpreted as the “expected number of exploited vulnerabilities.”

[0030] **Best Response Problems.** A pair of decision problems dealing with the best response for the players will now be described below. These problems are the deterministic host attacker problem (DHAP) and deterministic host defender problem (DHDP), respectively, and are defined as follows:

DHAP.

[0031] INPUT: $k_{atk} \in \mathbb{R}^+$, $x \in \mathbb{R}^+$, mixed defense strategy Pr_D , and payoff function p .

[0032] OUTPUT: “Yes” if $\exists A \in \mathbf{A}$ s.t. $\sum_{a \in A} c_a \leq k_{atk}$ and $\sum_{D \in \mathbf{D}} Pr_D(D) p(A, D) \geq x$, “No” otherwise.

DHDP.

[0033] INPUT: $x \in \mathbb{R}^+$, application constraints C , mixed attack strategy Pr_A , and payoff function p .

[0034] OUTPUT: “Yes” if $\exists D \in \mathbf{D}$ s.t. $\sum_{A \in \mathbf{A}} Pr_A(A) p(A, D) \leq x$ and D satisfies C . and “No” otherwise.

[0035] The natural optimization variants for these two problems will deal with maximizing the payoff in DHAP and minimizing the payoff in DHDP.

Analysis and Algorithms

[0036] The complexity and limits of approximation for both DHAP and DHDP will now be analyzed. The “Identity Exploit Model” is used for the complexity results. Unfortunately, both problems are NP-Complete in the general case.

[0037] **Theorem 1.** DHAP is NP-Complete, even when $|Pr_D|$ and the payoff function adheres to the submodularity and monotonicity axioms.

[0038] *Proof Sketch.* Membership in NP is trivial if the payoff is PTIME computable. The hardness result relies on an embedding of the well-known budgeted set cover. Here, the defender’s strategy is treated as a set of elements to

cover and the exploits are treated as subsets of D (by virtue of the exploit function). Exploit costs are set as 1 and the attacker's budget is the value budget from the embedded problem. So, the attacker must pick exploits to meet the budget and cover the determined number of the defender's vulnerabilities.0

[0039] Theorem 2. When $|C| > 1$ and $|Pr_A| = 1$, DHDP is NP-Complete.

[0040] Proof Sketch. Again, membership in NP is trivial if the payoff is PTIME computable. Hardness is shown by embedding the hitting set problem. In this reduction, the attacker plays all exploits and each exploit corresponds with precisely one vulnerability. This has the effect of imposing a unit cost on each vulnerability. Here, each C_i must be covered by a vulnerability. Hence, the defender must pick a set of all vulnerabilities to meet the cost requirement of DHDP while covering each C_i .

[0041] The hardness of approximation is also analyzed for the optimization variants of DHAP and DHDP. Due to the fact that the above embeddings used set cover and hitting set, we can draw upon the known past results to obtain the following corollaries:

[0042] Corollary 3. DHAP cannot be approximated where the payoff is within a factor of $(1 - \frac{1}{e})$ unless $P = NP$

[0043] Corollary 4. DHDP cannot be approximated where the payoff is within a factor of $(1 - o(1))\ln(n)$ unless $P = NP$

[0044] With the limits of approximation in mind, several algorithms are introduced to solve the optimization variants of DHAP and DHDP. The optimization variant of DHAP under the overlap payoff function is a special case of sub-modular maximization with the distinction that we are not simply picking k discrete objects, but instead picking items that each have a unique cost associated with them. Understanding this, several different approaches are examined to this problem based on the literature on submodular maximization. DHDP, on the other hand, can be readily approximated using the traditional set-cover algorithm (under some realistic assumptions), as cost does not affect DHDP.

Algorithm 1 Lazy Greedy Algorithm (Cost-Benefit Variant)

Input: $k_{atk} \in \mathbb{R}^+$, Pr_D , and payoff function p .

Output: $A \subseteq Ex$ such that $\sum_{a \in A} c_a \leq k_{atk}$

1. $A \leftarrow \emptyset$; $cost \leftarrow 0$; priority queue $Q \leftarrow \emptyset$; $iter \leftarrow 1$
 2. **for** $e \in Ex$ **do**
 3. $e.key \leftarrow \frac{\Delta_{p, Pr_D}(e | \emptyset)}{c_e}$; $e.i \leftarrow 1$
 4. Insert e into Q with $e.key$ as its key
 5. **end for**
 6. **while** $\{a \in Ex \setminus A : c_a + cost \leq k_{atk}\} \neq \emptyset$ **do**
 7. extract top (max) element e of Q
 8. **if** $e.i = iter$ and $c_e + cost \leq k_{atk}$ **then**
 9. $A \leftarrow A \cup \{e\}$; $iter \leftarrow iter + 1$
 10. $cost \leftarrow cost + c_e$
 11. **else if** $c_e + cost \leq k_{atk}$ **then**
 12. $e.i \leftarrow iter$; $e.key \leftarrow \frac{\Delta_{p, Pr_D}(e | A)}{c_e}$
 13. re-insert e into Q
 14. **end if**
 15. **end while**
 16. **return** A
-

Algorithms for DHAP

[0045] Greedy Approaches. As mentioned earlier, the non-unit cost of exploits mean that DHAP can be considered as a submodular maximization problem subject to knapsack constraints. Two versions of the traditional greedy algorithm can be applied: a cost-benefit variant and uniform-cost variant, both of which will also use the lazy-greedy optimization to further enhance performance while maintaining the approximation guarantee. It was independently noted that the uniform-cost and the cost-benefit algorithms can perform arbitrarily badly. However, by extending a result from either the cost-benefit or the uniform-cost algorithm will provide a solution within a factor of $\frac{1}{2}(1 - 1/e)$ for a given set of input parameters. By applying both algorithms to a given problem instance and returning the attack strategy which produces the larger payoff, the $\frac{1}{2}(1 - 1/e)$ approximation factor is achieved for DHAP. A cost-benefit lazy approximation algorithm is shown in Algorithm 1. By removing “ c_e ” from the denominator in the $e.key$ assignment in lines 3 and 12, the cost benefit lazy

approximation algorithm is transformed into a uniform cost lazy approximation algorithm.

[0046] Multiplicative Update Approach. An improved approximation ratio, when compared with the $\frac{1}{2}(1 - 1/e)$ ratio for the greedy algorithms, can be obtained by adapting Algorithm 1 for DHAP. This is shown as Algorithm 2 in this disclosure. For some value ϵ (a parameter), this algorithm provides a $(1 - \epsilon)(1 - 1/e)$ approximation of the optimal solution (Theorem 1.2), which, by providing an exceedingly small ϵ value, can get arbitrarily close to the $\frac{1}{2}(1 - 1/e)$ optimal approximation limit we discussed earlier.

Algorithm 2 Multiplicative Update

Input: $k_{atk}, \epsilon \in \mathbb{R}^+$ such that $0 < \epsilon < 1$, Pr_D , and payoff function p .

Output: $A \subseteq Ex$ s.t. $\sum_{a \in A} c_a \leq k_{atk}$

1. $Ex' \leftarrow \{ex \in Ex : c_{ex} \leq k_{atk}\}$
 2. $A \leftarrow \emptyset$
 3. $W \leftarrow \min_{ex'_i \in [Ex']} k_{atk}^2 / c_{ex'_i}$
 4. $w \leftarrow \frac{1}{k_{atk}}; \lambda \leftarrow e^{\frac{\epsilon W}{4}}$
 5. **while** $k_{atk}w \leq \lambda$ and $Ex' \neq \emptyset$ **do**
 6. $ex_j \leftarrow \operatorname{argmin}_{ex_j \in Ex' \setminus A} \left(\frac{c_{ex_j}}{k_{atk}} w / \Delta_{p, Pr_D}(ex_j | A) \right)$
 7. $A \leftarrow A \cup \{ex_j\}$
 8. $w \leftarrow w \lambda^{c_{ex_j} / k_{atk}^2}$
 9. $Ex' \leftarrow Ex' \setminus \{ex_j\}$
 10. **end while**
 11. **if** $\sum_{A_i \in A} c_{A_i} \leq k_{atk}$ **then**
 12. **return** A
 13. **else if** $\sum_{D \in Pr_D} Pr_D(D) p(A \setminus \{ex_j\}, D) \geq \sum_{D \in Pr_D} Pr_D(D) p(\{ex_j\}, D)$ **then**
 14. **return** $A \setminus \{ex_j\}$
 15. **else**
 16. **return** $\{ex_j\}$
 17. **end if**
-

[0047] Algorithm for DHDP. When using the overlap payoff function, DHDP can be modeled as a weighted set cover problem. Because the overlap payoff function is a modular function, the associated cost of a given vulnerability v , is simply the payoff produced by the singleton set $\{v\}$ with a mixed attack strategy. In the common case where each constraint set is a singleton set, if the overlap payoff

function is used, an adaptation on the standard greedy weighted set cover algorithm can be used for DHDP (Algorithm 3), providing a $\ln(n) + 1$ approximation,

Evaluation and Discussion

[0048] Darknet Market Data. Eight marketplaces located on the Tor network were scraped and parsed during the month of May 2015. Each of these markets host vendors offering “hacking tools”, including malware, botnets, exploits and other means serving to breach, steal and otherwise manipulate virtual targets. The product list is comprised of 235 such hacking tools, 167 of which were distinct.

Algorithm 3 Weighted Greedy DHDP Algorithm for Singleton Constraint Set and Overlap Payoff Case

Input: Vulnerabilities V , Pr_A , and application constraints $\mathcal{C}$

Output: $D \subseteq V$ s.t. the application constraints $\mathcal{C}$ are satisfied

1. $D \leftarrow \emptyset$
 2. $S \leftarrow \text{set such that } S_i = \{j : V_j \in \mathcal{C}_i \text{ where } V_j \text{ is the } i\text{th vulnerability in } V\}$
 3. $c_{S_i} \leftarrow \sum_{A \in Pr_A} Pr_A(A) |ExF(A) \cap \{V_i\}|$
 4. $\mathcal{C}' \leftarrow [\mathcal{C}]$
 5. **while** $\mathcal{C}' \neq \emptyset$ **do**
 6. $S_i \leftarrow \underset{S_i \in S}{\operatorname{argmax}} \frac{|S_i \cap \mathcal{C}'|}{c_{S_i}}$
 7. $\mathcal{C}' \leftarrow \mathcal{C}' \setminus S_i$
 8. $D \leftarrow D \cup \{V_i\}$
 9. **end while**
 10. **return** D
-

[0049] It found several identical products being sold on more than one market usually by the same seller (using an identical online handle). The products targeted 21 specific platforms, such as different versions of Adobe Flash, Linux, MSWindows and OS X as well as online presences such as Facebook, Wordpress and others. Hardware-related software such as those associated with Point-of-Sale machines, routers, and servers are also reflected in this number. FIG. 2 illustrates the variety of products in the markets and Table 2 illustrates exemplar exploits.

[0050] System Configurations. As noted in FIG. 2, a variety of platforms were represented in our darknet market data. Results are described using application constraints based on common configurations for Windows and Linux servers - as these were the most prominent targets of exploits found on the darknet. In our experiments, software was mapped such as media players, databases, and

FTP server software to application constraint sets to model the functional requirements of a system. Experiments were conducted with models for Android, Point-of-Sale, and Apple systems - though qualitatively the results differed little from the Windows and Linux Server experiments.

[0051] DHAP Results. Both the greedy and multiplicative update approaches were implemented to address the DHAP problem. For the greedy algorithm, three variants of greedy (cost-benefit, uniform cost, and combination of the two) were studied while we varied the parameter ϵ for the multiplicative update approach. Attacker payoff was examined as a function of budget (in Bitcoin). FIGS. **3A** and **3B** display this result. Though the cost-benefit greedy algorithm has the potential to perform poorly, it was, in general, the best performing approach - despite the multiplicative update approach achieving the better approximation guarantee. Further, the multiplicative update algorithm (Algorithm 2) was consistently the slowest in terms of runtime, taking much longer than the lazy greedy algorithms, particularly for high values of k_{atk} . Despite the multiplicative update algorithm having a better theoretical approximation ratio when compared to the tandem of greedy algorithms, namely $(1 - \epsilon) (1 - 1/e)$ compared to $\frac{1}{2}(1 - 1/e)$, as shown in FIGS. **3A** and **3B** that the greedy algorithms performed as good as or better than the multiplicative update very consistently. In all algorithms, as expected, runtime grew with budget (not pictured) - though the relationship was not strict, as an increase in budget does not necessarily mean that more exploits will be selected. In the experiments (on a commodity computer equipped with a 3.49 GHz i7 CPU and 16 GB of memory), the runtimes never exceeded ten minutes.

[0052] DHDP Results. FIGS. **4A** and **4B** demonstrate a defender's best response to an attack strategy against a Windows Server and Linux Server, respectively, for varying values of k_{atk} . Though similar trends are shown in FIGS. **3A** and **3B** as are shown in FIGS. **4A** and **4B**, the payoff is generally lower, meaning that the defender can lower the expected payoff by enacting a best response strategy to an attack strategy produced by DHAP - which in the framework translates to fewer exploited vulnerabilities.

[0053] Exploit Payoff Analysis. Instead of altering the software that appears on the host system in an attempt to avoid exploits, such as in the best response approach, in exploit payoff analysis, the defender will identify which specific exploits are increasing the payoff the most, with a hope that the defender

can reverse-engineer the exploit, or patch the vulnerability himself. To identify which exploits should be reverse-engineered, the defender first runs DHAP against his host system to identify what payoff an attacker could expect to produce. Then, for each exploit ex , the defender runs DHAP against the host with the set of exploits $Ex \setminus \{ex\}$. The exploit ex that, when removed from the universe of exploits Ex , produces the largest drop in payoff for the attacker is the exploit that the defender should attempt to reverse-engineer. More formally, let A be the attack strategy produced by DHAP when using Ex as the universe of exploits and let A_{ex} be the attack strategy that is produced when DHAP is run against the host when using $Ex \setminus \{ex\}$ as the universe of exploits. The defender will attempt to reverse-engineer the exploit, where D is the defense strategy representing the host. To account for exploits that, though they greatly reduce payoff when removed from Ex , may be too expensive for the defender to purchase, a cost-benefit analysis is also considered where the decrease in payoff is normalized by the cost of the exploit. The top exploits to reverse-engineer to defend a Windows Server host when considering an attacker budget of $k_{atk} = 5$, are shown in Table 3 with columns for both maximum payoff reduction and maximum cost-benefit analysis.

Prod.	Vuln.	Target	USD
Kernel Panic	X-display system	Linux < = 3.13.0-48	\$471.56
IE < = 11	memory corr.	IE on Windows < = 7	\$35.00
RemoteShell	wpconfig.php	Wordpress MU	\$1,500.00
0day RCE	WebView memory corr.	Android 4.1, 4.2	\$36.50
WindowsLPE	Win32k elev. of priv.	Windows < = 8.1	\$12.00-48.17
MS15-034 RCE	http.sys	Windows < = 8.1	\$311.97
FUD Flash Exp.	unspec.	FlashPlayer < = 16.0.0.287	\$600.00

Table 2: Examples of Exploits from Darknet Markets

Exploit	Max. Payoff Reduction	Max. Cost-Benefit	Exploit Cost (BTC)
SMTP Mail Cracker	1	4.757	0.2102
SUPEE-5433	1	1.190	0.8404
Hack ICQ	1	79.089	0.01264
Plasma	0.6677	1.582	0.2563
Wordpress Exploiter	0.6677	2.6467	0.2102
CVE-2014-0160	0.6677	3.178	0.2101

Table 3: Defender Exploit Analysis for $k_{atk} = 5$

Game Theoretic Framework

In some embodiments, to leverage the data collected from the darknet, a game theoretic framework is disclosed to reason about a defender facing an attacker

sourced through the communities on the darknet. The paradigm used for this is based on the framework of a “security game”. Such a framework 500 is designed from the ground-up to consider marketplace information a simplified block diagram is shown in FIG. 5. In this framework, an attacker has a strategy (denoted A) that consists of a set of exploits he must purchase within a given budget. An exploit function (denoted Ex) maps the attacker’s strategy to a set of vulnerable software applications, which can be easily obtained from darknet marketplace data. Meanwhile, the set of applications on a defender’s system D is treated as his strategy. While the payoff function is defined in terms of axioms, a simple payoff function can be the cardinality of the overlap -- $p(A, D) = |Ex(A) \cap D|$. The NP-hard problems of finding optimal strategies for both players and developed approximation algorithms are disclosed. A mixed strategy of attack and defense is disclosed that provides a natural extension for populations of computer systems as opposed to a single host as well as the modeling of multiple attackers.

[0054] Referring to FIG. 6, a detailed description of an example computing system 600 having one or more computing units that may implement various systems and methods discussed herein is provided. The computing system 600 may be applicable to the system described herein. For example, the computing system 600 may form a portion of the theoretical game engine 504 of FIG. 5 discussed above. It will be appreciated that specific implementations of these devices may be of differing possible specific computing architectures not all of which are specifically discussed herein but will be understood by those of ordinary skill in the art.

[0055] The computer system 600 may be a computing system is capable of executing a computer program product to execute a computer process. Data and program files may be input to the computer system 600, which reads the files and executes the programs therein. Some of the elements of the computer system 600 are shown in FIG. 6, including one or more hardware processors 602, one or more data storage devices 604, one or more memory devices 606, and/or one or more ports 608-612. Additionally, other elements that will be recognized by those skilled in the art may be included in the computing system 600 but are not explicitly depicted in Fig. 6 or discussed further herein. Various elements of the computer system 600 may communicate with one another by way of one or more

communication buses, point-to-point communication paths, or other communication means not explicitly depicted in FIG. 6.

[0056] The processor 602 may include, for example, a central processing unit (CPU), a microprocessor, a microcontroller, a digital signal processor (DSP), and/or one or more internal levels of cache. There may be one or more processors 602, such that the processor comprises a single central-processing unit, or a plurality of processing units capable of executing instructions and performing operations in parallel with each other, commonly referred to as a parallel processing environment.

[0057] The computer system 600 may be a conventional computer, a distributed computer, or any other type of computer, such as one or more external computers made available via a cloud computing architecture. The presently described technology is optionally implemented in software stored on the data stored device(s) 604, stored on the memory device(s) 606, and/or communicated via one or more of the ports 608-612, thereby transforming the computer system 600 in FIG. 6 to a special purpose machine for implementing the operations described herein. Examples of the computer system 600 include personal computers, terminals, workstations, mobile phones, tablets, laptops, personal computers, multimedia consoles, gaming consoles, set top boxes, and the like.

[0058] The one or more data storage devices 604 may include any non-volatile data storage device capable of storing data generated or employed within the computing system 600, such as computer executable instructions for performing a computer process, which may include instructions of both application programs and an operating system (OS) that manages the various components of the computing system 600. The data storage devices 604 may include, without limitation, magnetic disk drives, optical disk drives, solid state drives (SSDs), flash drives, and the like. The data storage devices 604 may include removable data storage media, non-removable data storage media, and/or external storage devices made available via a wired or wireless network architecture with such computer program products, including one or more database management products, web server products, application server products, and/or other additional software components. Examples of removable data storage media include Compact Disc Read-Only Memory (CD-ROM), Digital Versatile Disc Read-Only Memory (DVD-ROM), magneto-optical disks, flash drives, and the like. Examples of non-removable data storage media include

internal magnetic hard disks, SSDs, and the like. The one or more memory devices 606 may include volatile memory (e.g., dynamic random access memory (DRAM), static random access memory (SRAM), etc.) and/or non-volatile memory (e.g., read-only memory (ROM), flash memory, etc.).

[0059] Computer program products containing mechanisms to effectuate the systems and methods in accordance with the presently described technology may reside in the data storage devices 604 and/or the memory devices 606, which may be referred to as machine-readable media. It will be appreciated that machine-readable media may include any tangible non-transitory medium that is capable of storing or encoding instructions to perform any one or more of the operations of the present disclosure for execution by a machine or that is capable of storing or encoding data structures and/or modules utilized by or associated with such instructions. Machine-readable media may include a single medium or multiple media (e.g., a centralized or distributed database, and/or associated caches and servers) that store the one or more executable instructions or data structures.

[0060] In some implementations, the computer system 600 includes one or more ports, such as an input/output (I/O) port 608, a communication port 610, and a sub-systems port 612, for communicating with other computing, network, or vehicle devices. It will be appreciated that the ports 608-612 may be combined or separate and that more or fewer ports may be included in the computer system 600.

[0061] The I/O port 608 may be connected to an I/O device, or other device, by which information is input to or output from the computing system 600. Such I/O devices may include, without limitation, one or more input devices, output devices, and/or environment transducer devices.

[0062] In one implementation, the input devices convert a human-generated signal, such as, human voice, physical movement, physical touch or pressure, and/or the like, into electrical signals as input data into the computing system 600 via the I/O port 608. Similarly, the output devices may convert electrical signals received from computing system 600 via the I/O port 608 into signals that may be sensed as output by a human, such as sound, light, and/or touch. The input device may be an alphanumeric input device, including alphanumeric and other keys for communicating information and/or command selections to the processor 602 via the I/O port 608. The input device may be another type of user input device including, but not limited to: direction and selection control devices, such as a

mouse, a trackball, cursor direction keys, a joystick, and/or a wheel; one or more sensors, such as a camera, a microphone, a positional sensor, an orientation sensor, a gravitational sensor, an inertial sensor, and/or an accelerometer; and/or a touch-sensitive display screen ("touchscreen"). The output devices may include, without limitation, a display, a touchscreen, a speaker, a tactile and/or haptic output device, and/or the like. In some implementations, the input device and the output device may be the same device, for example, in the case of a touchscreen.

[0063] In one implementation, a communication port 610 is connected to a network by way of which the computer system 600 may receive network data useful in executing the methods and systems set out herein as well as transmitting information and network configuration changes determined thereby. Stated differently, the communication port 610 connects the computer system 600 to one or more communication interface devices configured to transmit and/or receive information between the computing system 600 and other devices by way of one or more wired or wireless communication networks or connections. For example, the computer system 600 may be instructed to access information stored in a public network, such as the Internet. The computer 600 may then utilize the communication port to access one or more publicly available servers that store information in the public network. In one particular embodiment, the computer system 600 uses an Internet browser program to access a publicly available website. The website is hosted on one or more storage servers accessible through the public network. Once accessed, data stored on the one or more storage servers may be obtained or retrieved and stored in the memory device(s) 606 of the computer system 600 for use by the various modules and units of the system, as described herein.

[0064] Examples of types of networks or connections of the computer system 600 include, without limitation, Universal Serial Bus (USB), Ethernet, Wi-Fi, Bluetooth®, Near Field Communication (NFC), Long-Term Evolution (LTE), and so on. One or more such communication interface devices may be utilized via the communication port 610 to communicate one or more other machines, either directly over a point-to-point communication path, over a wide area network (WAN) (e.g., the Internet), over a local area network (LAN), over a cellular (e.g., third generation (3G) or fourth generation (4G)) network, or over another communication means. Further,

the communication port 610 may communicate with an antenna for electromagnetic signal transmission and/or reception.

[0065] The computer system 600 may include a sub-systems port 612 for communicating with one or more additional systems to perform the operations described herein. For example, the computer system 600 may communicate through the sub-systems port 612 with a large processing system to perform one or more of the calculations discussed above.

[0066] The system set forth in FIG. 6 is but one possible example of a computer system that may employ or be configured in accordance with aspects of the present disclosure. It will be appreciated that other non-transitory tangible computer-readable storage media storing computer-executable instructions for implementing the presently disclosed technology on a computing system may be utilized.

[0067] FIG. 7 is a flowchart of a method for applying game theoretic cyber threat mitigation to a network. In one particular embodiment, the operations of the method 700 may be executed by the computing device described above in relation to FIG. 6. Thus, the computing device may utilize a network connection to a public network to obtain a set of exploits to attack a device or network, such as in operation 702. In some instances, the set of exploits may be obtained from the darknet portion of the Internet. In operation 704, the computing device creates a constraint set of vulnerabilities of a network under attack. In general, the constraint set of vulnerabilities includes those vulnerabilities in the attacked device or network that are required for some system functionality. In operation 706, the computing device applies the set of exploits to the constraint set of vulnerabilities of the attacked network to determine a success on attacking the network. In operation 708, the computing device may reverse engineer one or more of the set of exploits applied to the attacked network to develop a patch to the exposed vulnerability to the network.

[0068] It should be understood from the foregoing that, while particular embodiments have been illustrated and described, various modifications can be made thereto without departing from the spirit and scope of the invention as will be apparent to those skilled in the art. Such changes and modifications are within the scope and teachings of this invention as defined in the claims appended hereto.

Electronic Acknowledgement Receipt

EFS ID:	35749596
Application Number:	15362730
International Application Number:	
Confirmation Number:	5936
Title of Invention:	SYSTEMS AND METHODS FOR DATA DRIVEN GAME THEORETIC CYBER THREAT MITIGATION
First Named Inventor/Applicant Name:	Paulo Shakarian
Customer Number:	27148
Filer:	Ari M. Bai/Rebecca Endsley
Filer Authorized By:	Ari M. Bai
Attorney Docket Number:	055743-555439 M16-040P
Receipt Date:	17-APR-2019
Filing Date:	28-NOV-2016
Time Stamp:	11:38:22
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		555439_Response_to_Invitation_to_Correct.pdf	154676	yes	4
			e9c6bb553b307d24f51d3dc6586c66ccabf0adb0		

Multipart Description/PDF files in .zip description					
Document Description			Start	End	
Amendment after Notice of Allowance (Rule 312)			1	1	
Specification			2	3	
Applicant Arguments/Remarks Made in an Amendment			4	4	
Warnings:					
Information:					
2	Specification	555439_Marked_Up_Specification.pdf	483475	no	22
			4bd43539022767555b2043f97d822fcee4323b09		
Warnings:					
Information:					
3	Specification	555439_Substitute_Specification.pdf	291510	no	20
			624e0e46dfe7fadff9f7104db9fdb35d09ad37c3		
Warnings:					
Information:					
Total Files Size (in bytes):			929661		
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.
15/362,730	11/28/2016	Paulo Shakarian	055743-555439 M16-040P	5936
27148	7590	04/25/2019	EXAMINER	
POL SINELLI PC			TSANG, HENRY	
900 WEST 48TH PLACE				
SUITE 900				
KANSAS CITY, MO 64112-1895				
			ART UNIT	PAPER NUMBER
			2495	
			NOTIFICATION DATE	DELIVERY MODE
			04/25/2019	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):

patentdocketing@polsinelli.com
rendsley@polsinelli.com

Response to Rule 312 Communication	Application No. 15/362,730	Applicant(s)
	Examiner	Art Unit

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

1. ☒ The amendment filed on 17 April 2019 under 37 CFR 1.312 has been considered, and has been:

a) ☒ entered.

b) ☐ entered as directed to matters of form not affecting the scope of the invention.

c) ☐ disapproved because the amendment was filed after the payment of the issue fee.

Any amendment filed after the date the issue fee is paid must be accompanied by a petition under 37 CFR 1.313(c)(1) and the required fee to withdraw the application from issue.

d) ☐ disapproved. See explanation below.

e) ☐ entered in part. See explanation below.

Publishing Division

mn



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.
15/362,730	06/04/2019	10313385	055743-555439 M16-040P	5936

27148 7590 05/15/2019
POL SINELLI PC
900 WEST 48TH PLACE
SUITE 900
KANSAS CITY, MO 64112-1895

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 220 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):

Paulo Shakarian, Chandler, AZ;
ARIZONA BOARD OF REGENTS ON BEHALF OF ARIZONA STATE UNIVERSITY, Tempe, AZ
John Robertson, Prescott, AZ;
Jana Shakarian, Chandler, AZ;
Vivin Paliath, Chandler, AZ;
Amanda Thart, Scottsdale, AZ;

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.