(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 December 2016 (15.12.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/199128 A1

(51) International Patent Classification:
G06F 11/00 (2006.01) *G06F 12/14* (2006.01)

(21) International Application Number:
PCT/IL2016/050582

(22) International Filing Date:
6 June 2016 (06.06.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

62/172,251	8 June 2015 (08.06.2015)	US
62/172,253	8 June 2015 (08.06.2015)	US
62/172,255	8 June 2015 (08.06.2015)	US
62/172,259	8 June 2015 (08.06.2015)	US
62/172,261	8 June 2015 (08.06.2015)	US

(71) Applicant: **ILLUSIVE NETWORKS LTD.** [IL/IL]; 7 Tozeret Haaretz street, 6789104 Tel Aviv (IL).

(72) Inventors: **TOUBOUL, Shlomo**; 9 Beer Hamayim Street, Kfar Chaim 4294500 (IL). **LEVIN, Hanan**; 22 Ashkenazi street, Tel Aviv 6986440 (IL). **ROUBACH, Stephane**; 15 Chovot Halevavot Street, Herzliya 4632315 (IL). **MISCHARI, Assaf**; 11 Yael Rom Street, 4906207 Petach Tikva (IL). **BEN DAVID, Itai**; 29 Arlozorov Street, 6248804 Tel Aviv (IL). **AVRAHAM, Itay**; 181 Ben Yehuda Street, 6347210 Tel Aviv (IL). **OZER, Adi**; 22 Hasela Street, 6082253 Shoham (IL). **KAZAZ, Chen**; 10 Hamagid Street, 6522441 Tel Aviv (IL). **ISRAELI, Ofer**; 12 Ranak Street, 6346415 Tel Aviv (IL). **VINGURT, Olga**; 11 Havakouk Street, 8706611 Shderot (IL). **GAREH, Liad**; 4 Shvidelson Street, 4680704 Herzliya (IL). **GRIMBERG, Israel**; 14 Haprachim Street, 4339958 Raanana (IL). **COHEN, Cobby**; 7 Tozeret Haaretz Street, 6789104 Tel Aviv (IL). **SULTAN, Sharon**; 15 Brandeis Street, 6200121 Tel Aviv (IL). **KUBOVSKY, Matan**; 10 Bnei Dan Street, 6226005 Tel Aviv (IL).

(74) Agents: **GASSNER, Dvir** et al.; 55 Yigal Alon street, 6789115 Tel Aviv (IL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) Title: MULTI-FACTOR DECEPTION MANAGEMENT AND DETECTION FOR MALICIOUS ACTIONS IN A COMPUTER NETWORK

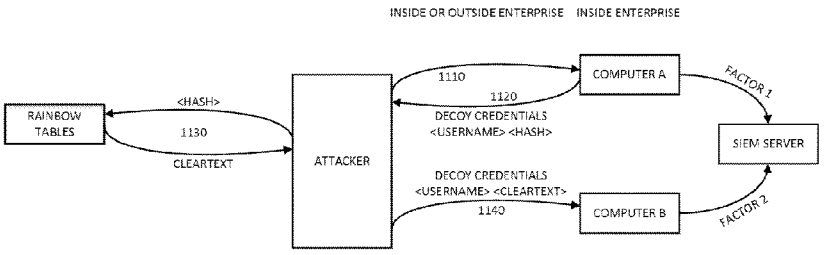

FIG. 3

(57) Abstract: A network surveillance system, including a management server within a network of resources in which users access the resources in the network based on credentials, including a deployment module planting honeytokens in resources in the network, wherein a honeytoken is an object in memory or storage of a first resource that may be used by an attacker to access a second resource using decoy credentials, and wherein the deployment module plants a first honeytoken in a first resource, *R1*, used to access a second resource, *R1*, using first decoy credentials, and plants a second honeytoken in *R2*, used to access a third resource, *R3*, using second decoy credentials, and an alert module alerting that an attacker is intruding the network only in response to both an attempt to access *R2* using the first decoy credentials, and a subsequent attempt to access *R3* using the second decoy credentials.

WO 2016/199128 A1

MULTI-FACTOR DECEPTION MANAGEMENT AND DETECTION FOR MALICIOUS ACTIONS IN A COMPUTER NETWORK

PRIORITY REFERENCES

[0001] This application claims benefit of and hereby incorporates by reference US Provisional Application No. 62/172,251, entitled SYSTEM AND METHOD FOR CREATION, DEPLOYMENT AND MANAGEMENT OF AUGMENTED ATTACKER MAP, and filed on June 8, 2015 by inventors Shlomo Touboul, Hanan Levin, Stephane Roubach, Assaf Mischari, Itai Ben David, Itay Avraham, Adi Ozer, Chen Kazaz, Ofer Israeli, Olga Vingurt, Liad Gareh, Israel Grimberg, Cobby Cohen and Sharon Sultan.

[0002] This application claims benefit of and hereby incorporates by reference US Provisional Application No. 62/172,253, entitled SYSTEM AND METHOD FOR MULTI-LEVEL DECEPTION MANAGEMENT AND DECEPTION SYSTEM FOR MALICIOUS ACTIONS IN A COMPUTER NETWORK, and filed on June 8, 2015 by inventors Shlomo Touboul, Hanan Levin, Stephane Roubach, Assaf Mischari, Itai Ben David, Itay Avraham, Adi Ozer, Chen Kazaz, Ofer Israeli, Olga Vingurt, Liad Gareh, Israel Grimberg, Cobby Cohen and Sharon Sultan.

[0003] This application claims benefit of and hereby incorporates by reference US Provisional Application No. 62/172,255, entitled METHODS AND SYSTEMS TO DETECT, PREDICT AND/OR PREVENT AN ATTACKER'S NEXT ACTION IN A COMPROMISED NETWORK, and filed on June 8, 2015 by inventors Shlomo Touboul, Hanan Levin, Stephane Roubach, Assaf Mischari, Itai Ben David, Itay Avraham, Adi Ozer, Chen Kazaz, Ofer Israeli, Olga Vingurt, Liad Gareh, Israel Grimberg, Cobby Cohen and Sharon Sultan.

[0004] This application claims benefit of and hereby incorporates by reference US Provisional Application No. 62/172,259, entitled MANAGING DYNAMIC DECEPTIVE ENVIRONMENTS, and filed on June 8, 2015 by inventors Shlomo Touboul, Hanan Levin, Stephane Roubach, Assaf Mischari, Itai Ben David, Itay Avraham, Adi Ozer, Chen Kazaz, Ofer Israeli, Olga Vingurt, Liad Gareh, Israel Grimberg, Cobby Cohen and Sharon Sultan.

[0005] This application claims benefit of and hereby incorporates by reference US Provisional Application No. 62/172,261, entitled SYSTEMS AND METHODS FOR AUTOMATICALLY GENERATING NETWORK ENTITY GROUPS BASED ON ATTACK PARAMETERS AND/OR ASSIGNMENT OF AUTOMATICALLY GENERATED SECURITY POLICIES, and filed on June 8, 2015 by inventors Shlomo Touboul, Hanan Levin, Stephane Roubach, Assaf Mischari, Itai Ben David, Itay Avraham, Adi Ozer, Chen Kazaz, Ofer Israeli, Olga Vingurt, Liad Gareh, Israel Grimberg, Cobby Cohen and Sharon Sultan.

FIELD OF THE INVENTION

[0006] The present invention relates to cyber security, and in particular to computer network surveillance.

BACKGROUND OF THE INVENTION

[0007] Reference is made to **FIG. 1**, which is a simplified diagram of a prior art enterprise network **100** connected to an external internet **10**. Network **100** is shown generally with resources including computers **110**, servers **120**, switches and routers **130**, and mobile devices **140** such as smart phones and tablets, for ease of presentation, although it will be appreciated by those skilled in the art that enterprise networks today are generally much more varied and complex and include other devices such as printers, phones and any Internet of Things objects. The various connections shown in **FIG. 1** may be direct or indirect, wired or wireless communications, or a combination of wired and wireless connections. Computers **110** and servers **120** may be physical elements or logical elements, or a mix of physical and logical elements. Computers **110** and servers **120** may be physical or virtual machines. Computer **110** and servers **120** may be local, remote or cloud-based elements, or a mix of local, remote and cloud-based elements. Computers **110** may be client workstation computers. Servers **120** may be file transfer protocol (FTP) servers, email servers, structured query language (SQL) servers, secure shell (SSH) servers, and other database and application servers. A corporate information technology (IT) department manages and controls network **100** in order to serve the corporate requirements and meet the corporate needs.

[0008] Access to computers **110** and servers **120** in network **100** may optionally be governed by an access governor **150**, such as a directory service, that authorizes users to access computers **110** and servers **120** based on "*credentials*" and other methods of authentication. Access governor **150** may be a name directory, such as ACTIVE DIRECTORY® developed by Microsoft Corporation of Redmond, WA, for WINDOWS® environments. Background information about ACTIVE DIRECTORY® is available at Wikipedia. Other access governors for WINDOWS and non-WINDOWS environments include inter alia Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), and Apple Filing Protocol (AFP), formerly APPLETALK®, developed by Apple Inc. of Cupertino, CA. Background information about LDAP, RADIUS and AFP is available at Wikipedia.

[0009] Access governor **150** may be one or more local machine access controllers. For networks that do not include an access governor, authentication may be performed by other servers **120**. Alternatively, in lieu of access governor **150**, resources of network **100** determine their local access rights.

[0010] Credentials for accessing computers **110** and servers **120** include inter alia server account credentials such as <address> <username> <password> for an FTP server, a database server, or an SSH server. Credentials for accessing computers **110** and servers **120** also include user login credentials <username> <password>, or <username> <ticket>, where "*ticket*" is an authentication ticket, such as a ticket for the Kerberos authentication protocol or NTLM hash used by Microsoft Corp., or login credentials via certificates or via another method of

authentication. Background information about the Kerberos protocol and LM hashes is available at Wikipedia.

[0011] Access governor **150** may maintain a directory of computers **110**, servers **120** and their users. Access governor **150** authorizes users and computers, assigns and enforces security policies, and installs and updates software.

[0012] Computers **110** may run a local or remote security service, which is an operating system process that verifies users logging in to computers, to other single sign-on systems, and to other credential storage systems.

[0013] Network **100** may include a security information and event management (SIEM) server **160**, which provides real-time analysis of security alerts generated by network hardware and applications. Background information about SIEM is available at Wikipedia.

[0014] Network **100** may include a domain name system (DNS) server **170**, or such other name service system, for translating domain names to IP addresses. Background information about DNS is available at Wikipedia.

[0015] Network **100** may include a firewall **180** located within a gateway between enterprise network **100** and external internet **10**. Firewall **180** controls incoming and outgoing traffic for network **100**. Background information about firewalls is available at Wikipedia.

[0016] One of the most prominent threats that organizations face is a targeted attack; i.e., an individual or group of individuals that attacks the organization for a specific purpose, such as stealing data, using data and systems, modifying data and systems, and sabotaging data and systems. Targeted attacks are carried out in multiple stages, typically including inter alia reconnaissance, penetration, lateral movement and payload.

Lateral movement involves orientation, movement and propagation, and includes establishing a foothold within the organization and expanding that foothold to additional systems within the organization.

[0017] In order to carry out the lateral movement stage, an attacker, whether a human being who is operating tools within the organization's network, or a tool with "*learning*" capabilities, learns information about the environment it is operating in, such as network topology, network devices and organization structure, learns "*where can I go from my current location*" and "*how can I get there from my current location (privilege required)*", learns implemented security solutions, learns applications that he can leverage, and then operates in accordance with that data.

[0018] An advanced attacker may use different attack techniques to enter a corporate network and to move laterally within the network in order to obtain its resource goals. The advanced attacker may begin with a workstation, server or any other network entity to start his lateral movement. He uses different methods to enter the network, including inter alia social engineering, existing exploit and/or vulnerability, and a Trojan horse or any other malware allowing him to control a first node or nodes.

[0019] Once an attacker has taken control of a first node in a corporate network, he uses different advanced attack techniques for orientation and propagation and discovery of additional ways to reach other network nodes in the corporate network. Attacker movement from node to node is performed via an "*attack vector*", which is an object discovered by the attacker, including inter alia an object in memory or storage of a first computer that may be used to access or discover a second computer.

[0020] Exemplary attack vectors include inter alia credentials of users with escalated privileges, existing share names on different servers and workstations, and details including address and credentials of an FTP server, an email server, a database server or an SSH server. Attack vectors are often available to an attacker because a user did not log off of his workstation, did not log out of an application, or did not clear his cache. E.g., if a user contacted a help desk and gave a help desk administrator remote access to his workstation, and if the help desk administrator did not properly log off from the remote access session to the users workstation, then the help desk access credentials may still be stored in the user's local cache and available to the attacker. Similarly, if the user accessed a server, e.g., an FTP server, then the FTP account login parameters may be stored in the user's local cache or profile and available to the attacker.

[0021] Attack vectors enable inter alia a move from workstation **A** → server **B** based on a shared server host name and its credentials, connection to a different workstation using local admin credentials that reside on a current workstation, and connection to an FTP server using specific access credentials.

[0022] Whereas IT "*sees*" the logical and physical network topology, an attacker that lands on a first network node "*sees*" attack vectors that depart from that node and move laterally to other nodes. The attacker can move to such nodes and then follow "*attack paths*" by successively discovering attack vectors from node to node.

[0023] When the attacker implements such a discovery process on all nodes in the network, he will be able to "*see*" all attack vectors of the corporate network and generate a "*complete attack map*". Before the

attacker discovers all attack vectors on network nodes and completes the discovery process, he generates a "*current attack map*" that is currently available to him.

[0024] An objective of the attacker is to discover an attack path that leads him to a target network node. The target may be a bank authorized server that is used by the corporation for ordering bank account transfers of money, it may be an FTP server that updates the image of all corporate points of sale, it may be a server or workstation that stores confidential information such as source code and secret formulas of the corporation, or it may be any other network nodes that are of value to the attacker and are his "*attack goal nodes*".

[0025] When the attacker lands on the first node, but does not know how to reach the attack goal node, he generates a current attack map that leads to the attack goal node.

[0026] One method to defend against such attacks, termed "*honeypots*", is to plant and monitor bait resources, with the objective that the attacker learn of their existence and then consume those bait resources, and to notify an administrator of the malicious activity. Background information about honeypots is available at Wikipedia.

[0027] Conventional honeypot systems operate by monitoring access to a supervised element in a computer network, the supervised element being a fake server or a fake service. Access monitoring generates many false alerts, caused by non-malicious access from automatic monitoring systems and by user mistakes. Conventional systems try to mitigate this problem by adding a level of interactivity to the honeypot, and by performing behavioral analysis of suspected malware if it has infected the honeypot itself.

SUMMARY

[0028] Embodiments of the present invention enhance confidence levels in identifying an attacker, by luring him into multiple access attempts to different resources monitored by the system, or into a single access attempt that requires multiple actions.

[0029] There is thus provided in accordance with an embodiment of the present invention a system for two-factor network surveillance to detect attackers, including a management server within a network of resources in which users access the resources in the network based on credentials, including a deployment module planting one or more honeytokens in one or more of the resources in the network, wherein a honeytoken is an object in memory or storage of a first resource that may be used by an attacker to access a second resource using decoy credentials, and wherein the deployment module plants a first honeytoken in a first resource, R_1, used to access a second resource, R_2, using first decoy credentials, and plants a second honeytoken in R_2, used to access a third resource, R_3, using second decoy credentials, and an alert module alerting that an attacker is intruding the network only in response to both (1) an attempt to access R_2 using the first decoy credentials, and (2) a subsequent attempt to access R_3 using the second decoy credentials.

[0030] There is additionally provided in accordance with an embodiment of the present invention a network surveillance method to detect attackers, including planting one or more honeytokens in one or more resources in a network of computers in which users access the resources in the network based on credentials, wherein a honeytoken is an object in memory or storage of a first resource that may be used by an attacker to access a second resource using decoy credentials, including planting a

first honeytoken in a first resource, R_1, used to access a second resource, R_2, using first decoy credentials, and planting a second honeytoken in R_2, used to access a third resource, R_3, using second decoy credentials, and alerting that an attacker is intruding the network only in response to both (i) an attempt to access R_2 using the first decoy credentials, and (ii) a subsequent attempt to access R_3 using the second decoy credentials.

[0031] There is further provided in accordance with an embodiment of the present invention a system for two-factor network surveillance to detect attackers, including a management server within a network of resources in which users access the resources in the network based on credentials, including a deployment module planting one or more honeytokens in one or more of the resources in the network, wherein a honeytoken is an object in memory or storage of a first resource that may be used by an attacker to access a second resource using decoy credentials, and wherein the deployment module plants a first honeytoken in a first resource, R_1, used to access a second resource, R_2, using first decoy credentials, and plants a second honeytoken in R_1, used to access a third resource, R_3, using second decoy credentials, and an alert module alerting that an attacker is intruding the network only in response to both (1) an attempt to access R_2 using the first decoy credentials, and (2) a subsequent attempt to access R_3 using the second decoy credentials.

[0032] There is yet further provided in accordance with an embodiment of the present invention a network surveillance method to detect attackers, including planting one or more honeytokens in one or more resources in a network of computers in which users access the resources in the network based on credentials, wherein a honeytoken is an object in memory or storage of a first resource that may be used by an attacker to

access a second resource using decoy credentials, including planting a first honeytoken in a first resource, R_1, used to access a second resource, R_2, using first decoy credentials and planting a second honeytoken in R_1, used to access a third resource, R_3, using second decoy credentials, and alerting that an attacker is intruding the network only in response to both (i) an attempt to access R_2 using the first decoy credentials, and (ii) a subsequent attempt to access R_3 using the second decoy credentials.

[0033] There is moreover provided in accordance with an embodiment of the present invention a system for two-factor network surveillance to detect attackers, including a management server within a network of resources, some of the resources being legitimate enterprise resources and others of the resources being decoy resources for the purpose of intrusion detection, the management server including a deployment module planting one or more honeytokens in one or more of the resources in the network, wherein a honeytoken is an object in memory or storage of a first resource that may be used by an attacker to discover existence of a second resource, and wherein said deployment module plants a first honeytoken in a resource, R, used to discover a first decoy resource, R_1, and plants a second honeytoken in R_1, used to discover a second decoy resource, R_2, and an alert module alerting that an attacker is intruding the network only in response to both (1) an attempt to access R_1, and (2) an attempt to access R_2.

[0034] There is additionally provided in accordance with an embodiment of the present invention a network surveillance method to detect attackers, including planting one or more honeytokens in one or more resources of a network of resources, some of the resources being legitimate enterprise resources and others of the resources being decoy

resources for the purpose of intrusion detection, wherein a honeytoken is an object in memory or storage of a first resource that may be used by an attacker to discover existence of a second resource, including planting a first honeytoken in a resource, R, used to discover a first decoy resource, R_1, and planting a second honeytoken in R_1, used to discover a second decoy resource, R_2, and alerting that an attacker is intruding the network only in response to both (i) an attempt to access R_1, and (ii) an attempt to access R_2.

[0035] There is further provided in accordance with an embodiment of the present invention a system for two-factor network surveillance to detect attackers, including a management server within a network of resources, some of the resources being legitimate enterprise resources and others of the resources being decoy resources for the purpose of intrusion detection, the management server including a deployment module planting one or more honeytokens in one or more of the resources in the network, wherein a honeytoken is an object in memory or storage of a first resource that may be used by an attacker to discover existence of a second resource, and wherein the deployment module plants a first honeytoken in a resource, R, used to discover a first decoy resource, R_1, and plants a second honeytoken in R, used to discover a second decoy resource, R_2, and an alert module alerting that an attacker is intruding the network only in response to both (1) an attempt to access R_1, and (2) an attempt to access R_2.

[0036] There is yet further provided in accordance with an embodiment of the present invention a network surveillance method to detect attackers, including planting one or more honeytokens in one or more resources of a network of resources, some of the resources being

legitimate enterprise resources and others of the resources being decoy resources for the purpose of intrusion detection, wherein a honeytoken is an object in memory or storage of a first resource that may be used by an attacker to discover existence of a second resource, including planting a first honeytoken in a resource, R, used to discover a first decoy resource, R_1, and planting a second honeytoken in R, used to discover a second decoy resource, R_2, and alerting that an attacker is intruding the network only in response to both (i) an attempt to access R_1, and (ii) an attempt to access R_2.

BRIEF DESCRIPTION OF THE DRAWINGS

[0037] The present invention will be more fully understood and appreciated from the following detailed description, taken in conjunction with the drawings in which:

[0038] **FIG. 1** is a simplified diagram of a prior art enterprise network connected to an external internet;

[0039] **FIG. 2** is a simplified diagram of an enterprise network with network surveillance, in accordance with an embodiment of the present invention;

[0040] **FIG. 3** is a simplified diagram of a method for network surveillance using two-factor deception, in accordance with an embodiment of the present invention;

[0041] **FIG. 4** is a simplified diagram of a method for network surveillance using two-factor deception, in accordance with an embodiment of the present invention;

[0042] **FIG. 5** is a simplified diagram of a method for network surveillance using multi-factor deception, in accordance with an embodiment of the present invention; and

[0043] **FIG. 6** is a simplified diagram of a method for network surveillance using multi-factor deception, in accordance with an embodiment of the present invention.

[0044] For reference to the figures, the following index of elements and their numerals is provided. Similarly numbered elements represent elements of the same type, but they need not be identical elements.

Table of elements in the figures	
Element	**Description**
10	Internet
100	enterprise network
110	network computers
120	network servers
130	network switches and routers
140	mobile devices
150	access governor (optional)
252	forensic alert module
160	SIEM server
170	DNS server
180	firewall
200	enterprise network with network surveillance
210	deception management server
211	policy manager
212	deployment module
213	forensic application
220	database of credential types
230	policy database
240	decoy servers
242	forensic alert module
260	update server

Elements numbered in the **1000**'s are operations of flow charts.

DETAILED DESCRIPTION

[0045] In accordance with embodiments of the present invention, systems and methods are provided for dynamically managing decoy policies for an enterprise network, which are planted in such a way as to increase confidence of detecting an attacker of the network, and to reduce false alerts.

[0046] Reference is made to **FIG. 2**, which is a simplified diagram of an enterprise network **200** with network surveillance, in accordance with an embodiment of the present invention. Network **200** includes a management server **210**, a database **220** of *"honeytokens"*, a policy database **230** and decoy servers **240**. In addition, network computers **110** and servers **120** are grouped into groups **G1**, **G2**, **G3** and **G4**. A *"honeytoken"* is data that may be used by an attacker to access a resource within network **200**, or merely to discover the existence of the resource without being able to access it. Symbolically **HT** → **R**, i.e., honeytoken **HT** provides a pointer to resource **R** within network **200**. Resource **R** may be inter alia (i) a computing device, such as a server computer or a router, or (ii) a service or application running on a computing device, such as an active directory service, a database application that accesses secure data, a financial application with transaction capability, a data transmission application, or a command and control application.

[0047] A honeytoken may be embodied as an object in memory or storage of a first resource within network **200** that may be used by an attacker to access a second resource within network **200**, or merely to discover the existence of a second resource without being able to access it. In some cases, the first and second resources reside on the same

computer, e.g., the second resource may be a service or application that requires a higher level of authentication than the first resource. A honeytoken may also be embodied as data, such as packet data, transmitted to or from a resource within network **200** or between resources within network **200**. An attacker generally uses honeytokens as clues within a treasure hunt.

[0048] The resource that a honeytoken points to may be (i) a real resource that exists within network **200**, e.g., an FTP server, (ii) a decoy resource that exists within network **200**, e.g., a decoy server **240**, or (iii) a resource that does not exist. In the latter case, when an attacker attempts to access a resource that does not exist, access governor **150** recognizes a pointer to a resource that is non-existent. Access governor **150** responds by notifying management server **210**, or by re-directing the pointer to a resource that does exist in order to survey the attacker's moves, or both.

[0049] Database **220** stores honeytokens that fake detection of and access to computers **110**, servers **120** and other resources in network **200**. Honeytokens include inter alia:

user names of the form <username>

user credentials of the form <username> <password>

user credentials of the form <username> <hash of password>

user credentials of the form <username> <ticket>

FTP server addresses of the form <FTP address>

FTP server credentials of the form <FTP address> <username> <password>

SSH server addresses of the form <SSH address>

SSH server credentials of the form <SSH address> <username> <password>

share addresses of the form <SMB address>

[0050] The honeytokens stored in database **220** are categorized by families, such as inter alia

F1 – user credentials

F2 - files

F3 – connections

F4 – FTP logins

F5 – SSH logins

F6 – share names

F7 – databases

F8 – network devices

F9 – URLs

F10 – Remote Desktop Protocol (RDP)

F11 – recent commands

F12 – scanners

F13 – cookies

F14 – cache

F15 – Virtual Private Network (VPN)

F16 – key logger

[0051] Database **220** communicates with an update server **260**, which updates database **220** as new types of honeytokens for detecting and accessing computers evolve over time, and as new algorithms for generating honeytokens arise. In addition to the honeytokens residing within database **200**, new honeytokens are also created dynamically.

[0052] Policy database **230** stores policies for planting honeytokens in computers of network **200**. Each policy specifies honeytokens that are planted in the computers, in accordance with honeytokens stored in database **220** and in accordance with new honeytokens that are dynamically generated. Honeytoken user credentials planted on a computer may lead to another resource in the network. Honeytokens to access an FTP, or other server, planted on a computer may lead to a decoy server **240**.

[0053] It will be appreciated by those skilled in the art the databases **220** and **230** may be combined into a single database, or distributed over multiple databases.

[0054] Management server **210** includes a policy manager **211**, a deployment module **212**, and a forensic application **213**. Policy manager **211** defines a decoy and response policy. The decoy and response policy defines different honeytoken types, different honeytoken combinations, response procedures, notification services, and assignments of policies to specific network nodes, network users, groups of nodes or users or both. Once policies are defined, they are stored in policy database **230** with the defined assignments.

[0055] In some embodiments of the present invention, some or all components of management server **210** may be integrated within an already existing enterprise deployment agent.

[0056] Deception management server **210** obtains the policies and their assignments from policy database **230**, and delivers them to appropriate nodes and groups. It then launches deployment module **212** to plant honeytoken on end points, servers, applications, routers, switches, relays and other entities in the network. Deployment module **212** plants each

honeytoken, based on its type, in memory (RAM), disk, or in any other data or information storage area, as appropriate, or as data, such as packet data, that is transmitted to or from a resource within network **200** or between resources of network **200**. Deployment module **212** plants the honeytokens in such a way that the chances of a valid user accessing the honeytokens are low. Deployment module **212** may or may not stay resident.

[0057] Forensic application **213** is a real-time application that is transmitted to a destination computer in the network, when a honeytoken is accessed by a computer **110**. When forensic application **213** is launched on the destination computer, it identifies a process running within that computer **110** that accessed that honeytoken, logs the activities performed by the thus-identified process in a forensic report, and transmits the forensic report to decoy management server **210**. Forensic application **213** also identifies and logs recent file activity, connection activity, background activity, and other time-based information that may be used to track an attacker's activity.

[0058] Once an attacker is detected, a "*response procedure*" is launched. The response procedure includes inter alia various notifications to various addresses, and actions on a decoy server such as launching an investigation process, and isolating, shutting down and re-imaging one or more network nodes. The response procedure collects information available on one or more nodes that may help in identifying the attacker's attack acts, intention and progress.

[0059] Each decoy server **240** includes a forensic alert module **242**, which creates a log and/or alerts management system **210** that an attacker is accessing the decoy server via a computer **110** of the

network, and causes management server **210** to send forensic application **213** to the computer that is accessing the decoy server. In an alternative embodiment of the present invention, decoy server **240** may store forensic application **213**, in which case decoy server **240** may transmit forensic application **213** directly to the computer that is accessing the decoy server. In another alternative embodiment of the present invention, management server **210** or decoy server **240** may transmit forensic application **213** to a destination computer other than the computer that is accessing the decoy server. Access governor **150** also activates a forensic alert module **252**, which creates a log and/or alerts management server **210** that an attacker is attempting to use a decoy credential.

[0060] Notification servers (not shown) are notified when an attacker uses a honeytoken. The notification servers may discover this by themselves, or by using information stored on access governor **150** and SIEM **160**. The notification servers forward notifications, or results of processing multiple notifications, to create notification time lines or such other analytics.

[0061] As mentioned above, conventional honeypot systems generate many false alerts. Embodiments of the present invention enhance confidence levels in identifying an attacker, by luring him into multiple access attempts to different resources monitored by the system, or into a single access attempt that requires multiple actions. The access attempts are comprised of multiple factors, each factor having a likelihood of being the intentional action of an attacker. **FIGS. 3 – 6** provide several embodiments of multi-factor deployment of honeytokens, as described below. Each factor may be inter alia an access attempt to a specific

resource, or an action performed in order to attempt access to a specific resource. Management server **210** issues an alert an alert only when two or more suspicious factors indicate an attack.

[0062] Reference is made to **FIG. 3**, which is a simplified diagram of a method for network surveillance using two-factor deception, in accordance with an embodiment of the present invention. At operation **1110** an attacker accesses a computer **A** of network **200**. At operation **1120** the attacker obtains a honeytoken with decoy credentials for accessing a computer **B** of network **200**, the decoy credentials being of the form <username> <hash>, where <hash> is a hash value of a cleartext password. The decoy credentials are preferably planted in computer **A** such that the chances of a valid user or automated monitor accessing the credentials are low.

[0063] At operation **1130** the attacker derives the cleartext password from <hash>. Operation **1130** may be performed by rainbow tables, which are pre-computed tables used by attackers for reversing cryptographic hash functions. At operation **1140** the attacker attempts a login to computer **B** using the cleartext version of the decoy credentials <username> <cleartext password>. At this stage, the chances of such login being performed by a valid user or automated monitor are extremely low, since this login requires two suspicious factors; namely, (i) extracting the decoy credentials with the hash value of the cleartext password from computer **A**, and (ii) reversing the extracted hash value to obtain the cleartext password. **FIG. 3** is an example of a single access that requires two actions.

[0064] It is noted in **FIG. 3** that an attacker may be located inside or outside the enterprise network. Embodiments of the present invention

monitor for malicious action regardless of whether the perpetrator is someone from inside or someone from outside of the enterprise.

[0065] Reference is made to **FIG. 4**, which is a simplified diagram of a method for network surveillance using two-factor deception, in accordance with an embodiment of the present invention. When an attacker discovers a honeytoken planted on a resource **A** with, say, a name of a server **S**, the attacker may retrieve the honeytoken data without attempting to access server **S** from resource **A**. The attacker may subsequently return to a different resource **B**, from which he tries to use the honeytoken data to access server **S**. As long as the honeytoken planted on resource **A** is unique to resource **A**, then the attack coming from resource **B** may be reliably identified, and diagnosed to conclude that the attacker's data was retrieved from resource **A**. As such, there are two incriminating factors; namely, (1) retrieval of the honeytoken from resource **A**, and (2) intrusion into resource **S**, and management server **210** issues an alert only when both factors have occurred.

[0066] Reference is made to **FIG. 5**, which is a simplified diagram of a method for network surveillance using multi-factor deception, in accordance with an embodiment of the present invention. With each successive intrusion of a resource, management server **210** provides a successive honeytoken from that resource to a next resource. The successive resources are structured so that the chances of a legitimate user accessing those resources are low.

[0067] The successive honeytokens are arranged such that each honeytoken may only be obtained after obtaining the previous ones, similar to successive clues in a treasure hunt, where one clue leads to the next. In the subject environment of intrusion detection, the clues are

decoys. Thus, referring to **FIG. 5**, honeytoken **2** → **C** can only be obtained when resource **B** is accessed via honeytoken **1** → **B**, and honeytoken **3** → **D** can only be obtained when resource **C** is accessed via honeytoken **2** → **C**. Each access to a resource is reported to SIEM server **160**, allowing for evaluation of a confidence level that a suspected attacker is indeed a malicious attacker. The successive access attempts continue by providing the suspected attacker with successive honeytokens pointing at previously used or new resources, until a threshold confidence level is reached. Management server **210** issues an alert only when three access attempts have occurred.

[0068] Resources **A**, **B**, **C** and **D** in **FIG. 5** may reside on different computers, or on the same computer. E.g., resources **A**, **B**, **C**, **D** may be services or applications running on the same computer that require different levels of authentication.

[0069] As explained with reference to **FIG. 4** above, the attack on resource **B** shown in **FIG. 5** may be via resource **A**, or via a different resource using honeytoken **1** → **B**. Similarly for the attacks on resources **C** and **D**.

[0070] Reference is made to **FIG. 6**, which is a simplified diagram of a method for network surveillance using multi-factor deception, in accordance with an embodiment of the present invention. Three honeytoken attack vectors are planted on resource **A**; namely, honeytoken **1** → **B**, honeytoken **2** → **C**, honeytoken **3** → **D**. Each use of a honeytoken is reported to SIEM server **160**, allowing for evaluation of a confidence level that the resources are being accessed by a malicious attacker. Management server **210** issues an alert only three access attempts have occurred.

[0071] As explained with reference to **FIG. 4** above, the attack on resource **B** shown in **FIG. 5** may be via resource **A**, or via a different resource using honeytoken **1** → **B**. Similarly for the attacks on resources **C** and **D**.

[0072] When an attacker discovers a honeytoken with a name and credentials of a resource, the attacker may nevertheless attempt accessing the resource with different credentials or via an exploit.

[0073] In the foregoing specification, the invention has been described with reference to specific exemplary embodiments thereof. It will, however, be evident that various modifications and changes may be made to the specific exemplary embodiments without departing from the broader spirit and scope of the invention. Accordingly, the specification and drawings are to be regarded in an illustrative rather than a restrictive sense.

CLAIMS

What is claimed is:

1. A system for two-factor network surveillance to detect attackers, comprising:

a management server within a network of resources in which users access the resources in the network based on credentials, comprising a deployment module planting one or more honeytokens in one or more of the resources in the network, wherein a honeytoken is an object in memory or storage of a first resource that may be used by an attacker to access a second resource using decoy credentials, and wherein said deployment module plants a first honeytoken in a first resource, R_1, used to access a second resource, R_2, using first decoy credentials, and plants a second honeytoken in R_2, used to access a third resource, R_3, using second decoy credentials; and

an alert module alerting that an attacker is intruding the network only in response to both (1) an attempt to access R_2 using the first decoy credentials, and (2) a subsequent attempt to access R_3 using the second decoy credentials.

2. The system of claim **1** wherein some of the resources are legitimate enterprise resources and others of the resources are decoy resources for the purpose of intrusion detection, and wherein resources R_2 and R_3 comprise decoy resources.

3. The system of claim **1** wherein credentials include passwords for accessing resources in the network, and wherein the first and second

decoy credentials include respective hash versions of first and second passwords.

4. The system of claim **1** wherein credentials of honeytokens include members of the group consisting of user credentials, FTP server credentials and SSH server credentials.

5. A network surveillance method to detect attackers, comprising:

planting one or more honeytokens in one or more resources in a network of computers in which users access the resources in the network based on credentials, wherein a honeytoken is an object in memory or storage of a first resource that may be used by an attacker to access a second resource using decoy credentials, comprising:

planting a first honeytoken in a first resource, R_1, used to access a second resource, R_2, using first decoy credentials; and

planting a second honeytoken in R_2, used to access a third resource, R_3, using second decoy credentials; and

alerting that an attacker is intruding the network only in response to both (i) an attempt to access R_2 using the first decoy credentials, and (ii) a subsequent attempt to access R_3 using the second decoy credentials.

6. The method of claim **5** wherein credentials include passwords for accessing resources in the network, and wherein the first and second decoy credentials include respective hash versions of first and second passwords.

7. The method of claim **5** wherein credentials of honeytokens include members of the group consisting of user credentials, FTP server credentials and SSH server credentials.

8. A system for two-factor network surveillance to detect attackers, comprising:

a management server within a network of resources in which users access the resources in the network based on credentials, comprising a deployment module planting one or more honeytokens in one or more of the resources in the network, wherein a honeytoken is an object in memory or storage of a first resource that may be used by an attacker to access a second resource using decoy credentials, and wherein said deployment module plants a first honeytoken in a first resource, R_1, used to access a second resource, R_2, using first decoy credentials, and plants a second honeytoken in R_1, used to access a third resource, R_3, using second decoy credentials; and

an alert module alerting that an attacker is intruding the network only in response to both (1) an attempt to access R_2 using the first decoy credentials, and (2) a subsequent attempt to access R_3 using the second decoy credentials.

9. The system of claim **8** wherein some of the resources are legitimate enterprise resources and others of the resources are decoy resources for the purpose of intrusion detection, and wherein resources R_2 and R_3 comprise decoy resources.

10. The system of claim **8** wherein credentials include passwords for accessing resources in the network, and wherein the first and second decoy credentials include respective hash versions of first and second passwords.

11. The system of claim **8** wherein credentials of honeytokens include members of the group consisting of user credentials, FTP server credentials and SSH server credentials.

12. A network surveillance method to detect attackers, comprising:

planting one or more honeytokens in one or more resources in a network of computers in which users access the resources in the network based on credentials, wherein a honeytoken is an object in memory or storage of a first resource that may be used by an attacker to access a second resource using decoy credentials, comprising:

planting a first honeytoken in a first resource, R_1, used to access a second resource, R_2, using first decoy credentials; and

planting a second honeytoken in R_1, used to access a third resource, R_3, using second decoy credentials; and

alerting that an attacker is intruding the network only in response to both (i) an attempt to access R_2 using the first decoy credentials, and (ii) a subsequent attempt to access R_3 using the second decoy credentials.

13. The method of claim **12** wherein credentials include passwords for accessing resources in the network, and wherein the first and second

decoy credentials include respective hash versions of first and second passwords.

14. The method of claim **12** wherein credentials of honeytokens include members of the group consisting of user credentials, FTP server credentials and SSH server credentials.

15. A system for two-factor network surveillance to detect attackers, comprising:

a management server within a network of resources, some of the resources being legitimate enterprise resources and others of the resources being decoy resources for the purpose of intrusion detection, the management server comprising a deployment module planting one or more honeytokens in one or more of the resources in the network, wherein a honeytoken is an object in memory or storage of a first resource that may be used by an attacker to discover existence of a second resource, and wherein said deployment module plants a first honeytoken in a resource, R, used to discover a first decoy resource, R_1, and plants a second honeytoken in R_1, used to discover a second decoy resource, R_2; and

an alert module alerting that an attacker is intruding the network only in response to both (1) an attempt to access R_1, and (2) an attempt to access R_2.

16. A network surveillance method to detect attackers, comprising:

planting one or more honeytokens in one or more resources of a network of resources, some of the resources being legitimate enterprise resources and others of the resources being decoy resources for the purpose of intrusion detection, wherein a honeytoken is an object in memory or storage of a first resource that may be used by an attacker to discover existence of a second resource, comprising:

planting a first honeytoken in a resource, R, used to discover a first decoy resource, R_1; and

planting a second honeytoken in R_1, used to discover a second decoy resource, R_2; and

alerting that an attacker is intruding the network only in response to both (i) an attempt to access R_1, and (ii) an attempt to access R_2.

17. A system for two-factor network surveillance to detect attackers, comprising:

a management server within a network of resources, some of the resources being legitimate enterprise resources and others of the resources being decoy resources for the purpose of intrusion detection, the management server comprising a deployment module planting one or more honeytokens in one or more of the resources in the network, wherein a honeytoken is an object in memory or storage of a first resource that may be used by an attacker to discover existence of a second resource, and wherein said deployment module plants a first honeytoken in a resource, R, used to discover a first decoy resource, R_1, and plants a second honeytoken in R, used to discover a second decoy resource, R_2; and

an alert module alerting that an attacker is intruding the network only in response to both (1) an attempt to access R_1, and (2) an attempt to access R_2.

18. A network surveillance method to detect attackers, comprising:

planting one or more honeytokens in one or more resources of a network of resources, some of the resources being legitimate enterprise resources and others of the resources being decoy resources for the purpose of intrusion detection, wherein a honeytoken is an object in memory or storage of a first resource that may be used by an attacker to discover existence of a second resource, comprising:

planting a first honeytoken in a resource, R, used to discover a first decoy resource, R_1; and

planting a second honeytoken in R, used to discover a second decoy resource, R_2; and

alerting that an attacker is intruding the network only in response to both (i) an attempt to access R_1, and (ii) an attempt to access R_2.

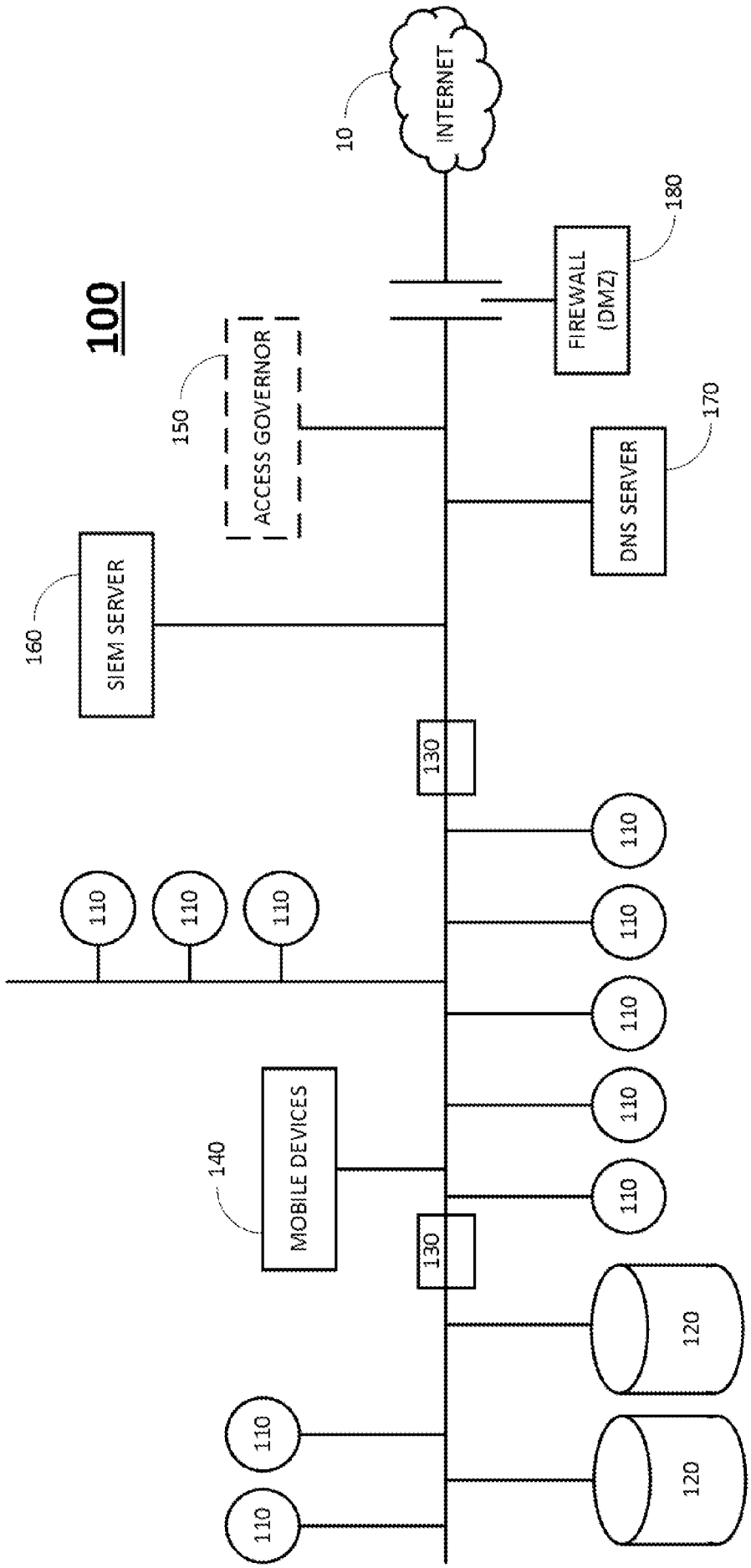

FIG. 1
(PRIOR ART)

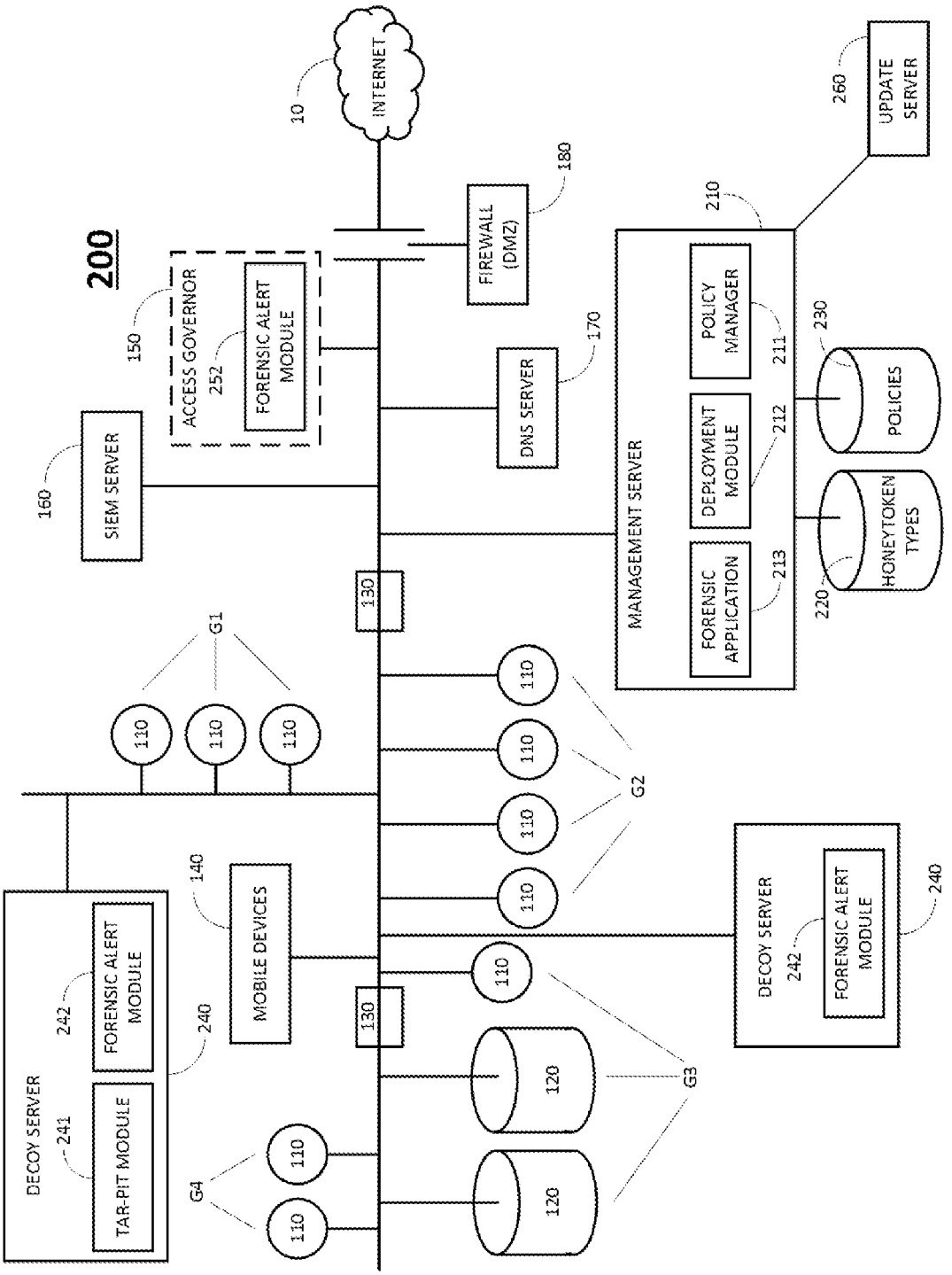
200
10
INTERNET
260
UPDATE SERVER
210
MANAGEMENT SERVER
POLICY MANAGER
211
DEPLOYMENT MODULE
212
FORENSIC APPLICATION
213
230
POLICIES
220
HONEYTOKEN TYPES
180
FIREWALL (DMZ)
170
DNS SERVER
150
ACCESS GOVERNOR
252
FORENSIC ALERT MODULE
160
SIEM SERVER
130
130
G1
G2
G3
G4
110
120
140
MOBILE DEVICES
DECOY SERVER
241
TAR-PIT MODULE
242
FORENSIC ALERT MODULE
240
DECOY SERVER
242
FORENSIC ALERT MODULE
240

FIG. 2

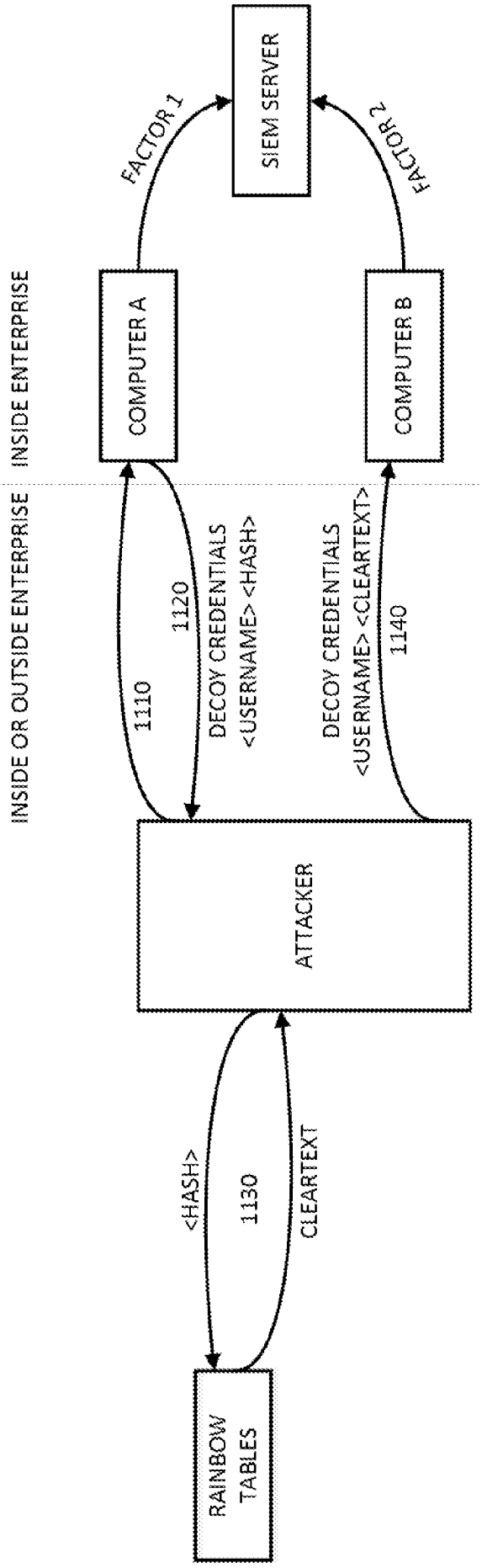
SIEM SERVER
FACTOR 1
FACTOR 2
INSIDE ENTERPRISE
INSIDE OR OUTSIDE ENTERPRISE
COMPUTER A
COMPUTER B
1110
1120
DECOY CREDENTIALS
<USERNAME> <HASH>
DECOY CREDENTIALS
<USERNAME> <CLEARTEXT>
1140
ATTACKER
<HASH>
1130
CLEARTEXT
RAINBOW TABLES

FIG. 3

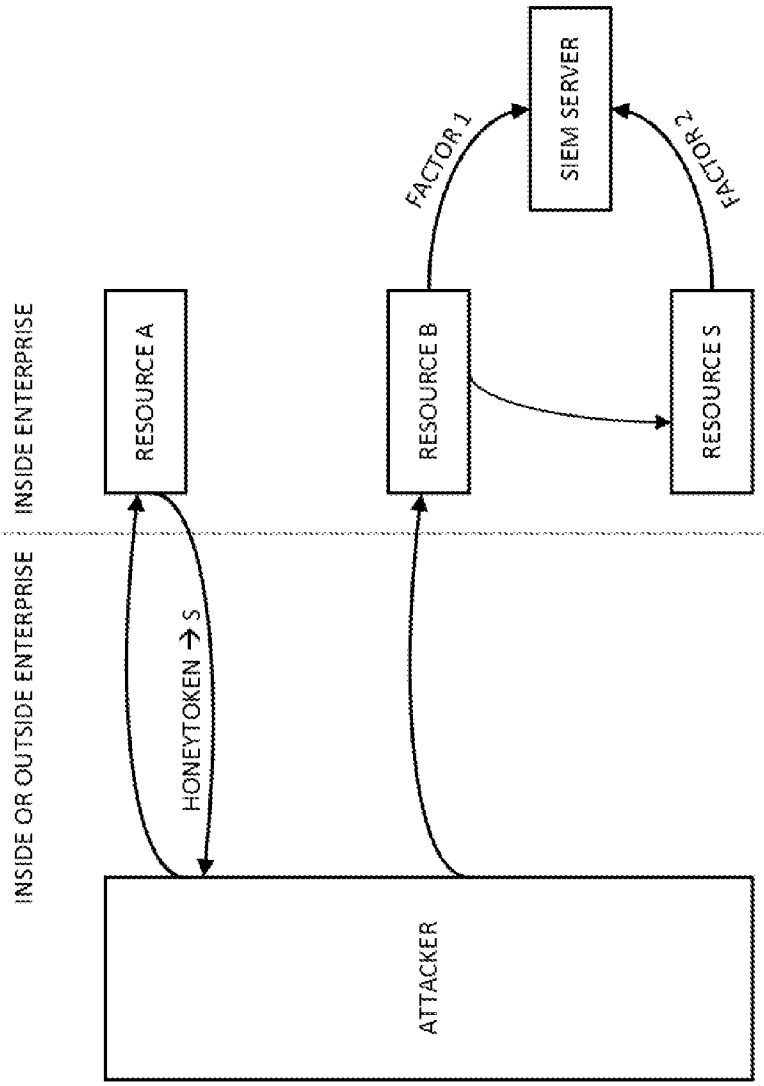
INSIDE ENTERPRISE
INSIDE OR OUTSIDE ENTERPRISE
RESOURCE A
RESOURCE B
RESOURCE S
SIEM SERVER
FACTOR 1
FACTOR 2
HONEYTOKEN → S
ATTACKER

FIG. 4

4/6

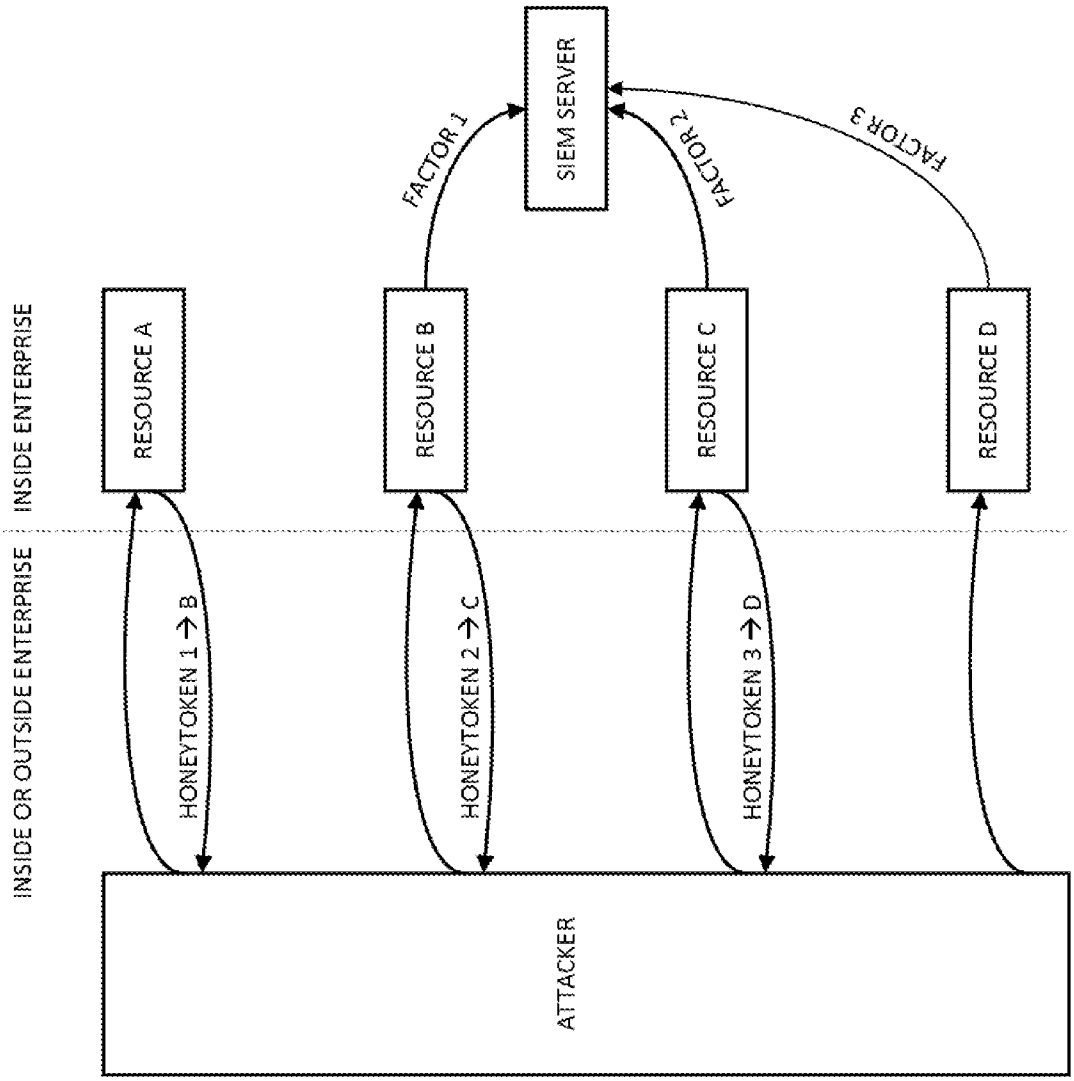
INSIDE OR OUTSIDE ENTERPRISE
INSIDE ENTERPRISE
RESOURCE A
RESOURCE B
RESOURCE C
RESOURCE D
SIEM SERVER
FACTOR 1
FACTOR 2
FACTOR 3
HONEYTOKEN 1 → B
HONEYTOKEN 2 → C
HONEYTOKEN 3 → D
ATTACKER

FIG. 5

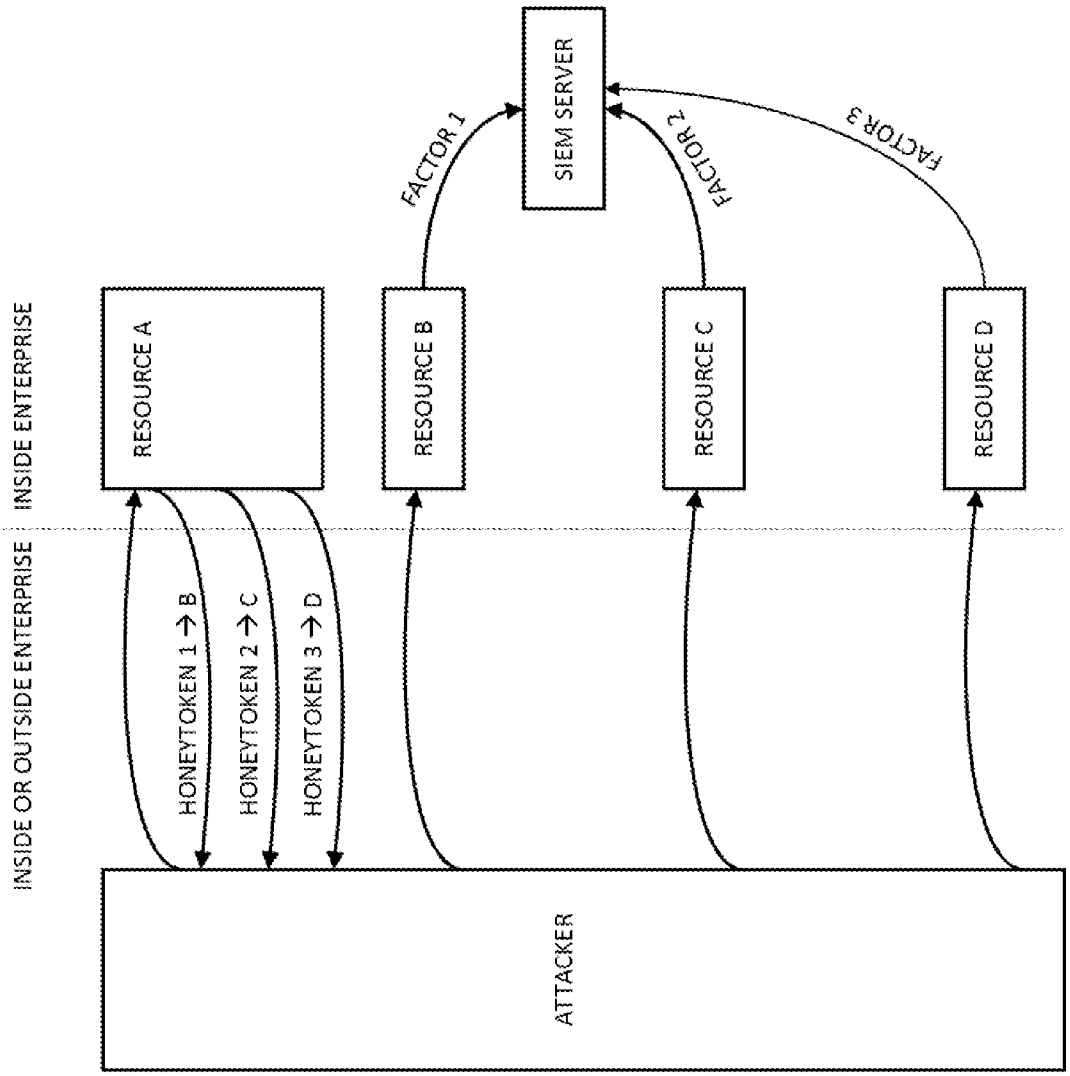
INSIDE ENTERPRISE
INSIDE OR OUTSIDE ENTERPRISE
RESOURCE A
RESOURCE B
RESOURCE C
RESOURCE D
SIEM SERVER
FACTOR 1
FACTOR 2
FACTOR 3
HONEYTOKEN 1 → B
HONEYTOKEN 2 → C
HONEYTOKEN 3 → D
ATTACKER

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL 16/50582

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 11/00, G06F 12/14 (2016.01)
CPC - H04L 63/1408
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8): G06F 11/00, G06F 12/14 (2016.01)
CPC: H04L 63/1408

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 726/22, 726/23, 726/24, 726/25, 726/26 (Keyword limited; terms below); IPC(8): G06F 11/00, G06F 12/14 (2016.01) (Keyword limited; terms below); CPC: H04L 63/1416, H04L 63/1408, H04L 63/145, H04L 63/1441, H04L 63/1458 (Keyword limited; terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase; Google (Scholar, Patents, Web)
Terms used: honeytoken decoy credential detect intrusion attempt password hash ftp ssh

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012/0084866 A1 (STOLFO), 05 April 2012 (05.04.2012), entire document, especially Abstract; para [0045], [0099], [0110], [0120], [0183]-[0185], [0191]	1-18
A	US 2009/0328216 A1 (RAFALOVICH et al.), 31 December 2009 (31.12.2009), entire document	1-18
A	US 2015/0013006 A1 (SCHULMAN et al.), 08 January 2015 (08.01.2015), entire document	1-18
A	WO 2015/047555 A1 (ATHANASOPOULOS et al.), 04 February 2015 (04.02.2015), entire document	1-18

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 October 2016	16 NOV 2016
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774