(21) International Application Number: PCT/US20 160/17862

(22) International Filing Date: 12 February 2016 (12.02.2016)

(25) Filing Language: English

(26) Publication Language: English


(72) Inventors: SANDER, Tomas; 5 Vaughan Drive, Suite 301, Princeton, New Jersey 08540 (US). HEIN, Brian Frederik Hosea Che; 2341 1 Summerfield #37a, Aliso Viejo, California 92656 (US). COHEN, Nadav; 1160 Enterprise Way, Sunnyvale, California 94089 (US). ROSS, Ted; 1423 1 Tandem Boulevard, Austin, Texas 78728 (US).


(51) International Patent Classification: H04L 29/06 (2006.01) H04L 12/22 (2006.01)

(54) Title: SOURCE ENTITIES OF SECURITY INDICATORS

(57) Abstract: Examples disclosed herein relate to source entities of security indicators. Some examples disclosed herein enable identifying, in a security information sharing platform, a security indicator that is originated from a source entity where the security indicator comprises an observable. Some examples further enable determining a reliability level of the source entity based on at least one of: security events, sightings of the observable, a first set of user feedback information that is submitted for the security indicator by users of the security information sharing platform, or a second set of user feedback information that is collected from external resources that are external to the security information sharing platform.

FIG. 5
as to applicant’s entitlement to apply for and be granted a patent (Rule 4.17(ii))

Published.

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

[0001] Users of a security information sharing platform share security indicators, security alerts, and/or other security-related information (e.g., mitigations strategies, attackers, attack campaigns and trends, threat intelligence information, etc.) with other users in an effort to advise the other users of any security threats, or to gain information related to security threats from other users.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] The following detailed description references the drawings, wherein:

[0003] FIG. 1 is a block diagram depicting an example environment in which various examples may be implemented as a source entities system.
[0004] FIG. 2 is a block diagram depicting an example source entities system.
[0005] FIG. 3 is a block diagram depicting an example machine-readable storage medium comprising instructions executable by a processor for source entities of security indicators.
[0006] FIG. 4 is a block diagram depicting an example machine-readable storage medium comprising instructions executable by a processor for source entities of security indicators.
[0007] FIG. 5 is a flow diagram depicting an example method for determining reliability levels of source entities of security indicators.
[0008] FIG. 6 is a flow diagram depicting an example method for determining reliability and authenticity levels of source entities of security indicators.
DETAILED DESCRIPTION

[0009] The following detailed description refers to the accompanying drawings. Wherever possible, the same reference numbers are used in the drawings and the following description to refer to the same or similar parts. It is to be expressly understood, however, that the drawings are for the purpose of illustration and description only. While several examples are described in this document, modifications, adaptations, and other implementations are possible. Accordingly, the following detailed description does not limit the disclosed examples. Instead, the proper scope of the disclosed examples may be defined by the appended claims.

[0010] Users of a security information sharing platform share security indicators, security alerts, and/or other security-related information (e.g., mitigations strategies, attackers, attack campaigns and trends, threat intelligence information, etc.) with other users in an effort to advise the other users of any security threats, or to gain information related to security threats from other users. The other users with whom the security information is shared typically belong to a community that is selected by the user for sharing, or to the same community as the user. The other users of such communities may further share the security information with further users and/or communities. A "user," as used herein, may include an individual, organization, or any entity that may send, receive, and/or share the security information. A community may include a plurality of users. For example, a community may include a plurality of individuals in a particular area of interest. A community may include a global community where any user may join, for example, via subscription. A community may also be a vertical-based community. For example, a vertical-based community may be a healthcare or a financial community. A community may also be a private community with a limited number of selected users.

[0011] A "security indicator," as used herein, may refer to a detection guidance for a security threat and/or vulnerability. In other words, the security indicator may specify what to detect or look for (e.g., an observable) and/or what it means if detected. For example, the security indicator may specify a certain Internet Protocol (IP) address to look for in the network traffic. The security indicator may
include the information that the detection of that IP address in the network traffic can indicate a certain malicious security threat such as a Trojan virus. A security indicator may be created by and/or originated from at least one of a plurality of source entities. For example, the plurality of source entities may include a user (e.g., analysts and/or community members of the security information sharing platform). A security indicator may be manually created and/or added to the security information sharing platform by the user. In another example, the plurality of source entities may include a threat intelligence provider that provides threat intelligence feeds and/or any other participating organizations. A security indicator that is found in the intelligence feeds and/or information from other participating organizations, for example, may be automatically created and/or added to the security information sharing platform.

[0012] Since security indicators can be easily created and/or added by various source entities using the security information sharing platform, there may be a risk that a certain security indicator is erroneously classified as malicious that poses an actual security threat. For example, if a popular news site that is actually benign and not malicious is included as an observable in a security indicator, the site can be blocked, causing inconvenience to the users and/or communities. Moreover, this may cause erroneous security alerts to be generated, contaminating the data being shared and continuously being re-shared in the security information sharing environment.

[0013] Examples disclosed herein provide technical solutions to these technical challenges by determining a reliability level and/or an authenticity level of a source entity of a particular security indicator to help determine an indicator score associated the particular security indicator. Accurate indicator scores help prioritize among a large amount of data maintained by the security information sharing platform to enable an informed and timely decision on threat mitigation. Source reliability and/or authenticity are important ingredients for computing accurate indicator scores. For example, threat intelligence from an organization with a track record for skilled and competent analysis can be trusted more than threat intelligence from another organization with a low reputation.
Some examples disclosed herein enable identifying, in a security information sharing platform, a security indicator that is originated from a source entity where the security indicator comprises an observable. Some examples further enable determining a reliability level of the source entity based on at least one of: security events, sightings of the observable, a first set of user feedback information that is submitted for the security indicator by users of the security information sharing platform, or a second set of user feedback information that is collected from external resources that are external to the security information sharing platform.

The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting. As used herein, the singular forms "a," "an," and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. The term "plurality," as used herein, is defined as two or more than two. The term "another," as used herein, is defined as at least two or more. The term "coupled," as used herein, is defined as connected, whether directly without any intervening elements or indirectly with at least one intervening elements, unless otherwise indicated. Two elements can be coupled mechanically, electrically, or communicatively linked through a communication channel, pathway, network, or system. The term "and/or" as used herein refers to and encompasses any and all possible combinations of one or more of the associated listed items. It will also be understood that, although the terms first, second, third, etc. may be used herein to describe various elements, these elements should not be limited by these terms, as these terms are only used to distinguish one element from another unless stated otherwise or the context indicates otherwise. As used herein, the term "includes" means includes but not limited to, the term "including" means including but not limited to. The term "based on" means based at least in part on.

FIG. 1 is an example environment 100 in which various examples may be implemented as a source entities system 110. Environment 100 may include various components including server computing device 130 and client computing devices 140 (illustrated as 140A, 140B, ..., 140N). Each client computing device 140A, 140B, ..., 140N may communicate requests to and/or receive responses
from server computing device 130. Server computing device 130 may receive and/or respond to requests from client computing devices 140. Client computing devices 140 may be any type of computing device providing a user interface through which a user can interact with a software application. For example, client computing devices 140 may include a laptop computing device, a desktop computing device, an all-in-one computing device, a tablet computing device, a mobile phone, an electronic book reader, a network-enabled appliance such as a "Smart" television, and/or other electronic device suitable for displaying a user interface and processing user interactions with the displayed interface. While server computing device 130 is depicted as a single computing device, server computing device 130 may include any number of integrated or distributed computing devices serving at least one software application for consumption by client computing devices 140.

[0017] The various components (e.g., components 129, 130, and/or 140) depicted in FIG. 1 may be coupled to at least one other component via a network 50. Network 50 may comprise any infrastructure or combination of infrastructures that enable electronic communication between the components. For example, network 50 may include at least one of the Internet, an intranet, a PAN (Personal Area Network), a LAN (Local Area Network), a WAN (Wide Area Network), a SAN (Storage Area Network), a MAN (Metropolitan Area Network), a wireless network, a cellular communications network, a Public Switched Telephone Network, and/or other network. According to various implementations, source entities system 110 and the various components described herein may be implemented in hardware and/or a combination of hardware and programming that configures hardware. Furthermore, in FIG. 1 and other Figures described herein, different numbers of components or entities than depicted may be used.

[0018] Source entities system 110 may comprise a security indicator engine 121, a sighting engine 122, a source reliability engine 123, a source authenticity engine 124, an indicator score engine 125, and/or other engines. The term "engine", as used herein, refers to a combination of hardware and programming that performs a designated function. As is illustrated respect to FIGS. 3-4, the hardware of each engine, for example, may include one or both of a processor
and a machine-readable storage medium, while the programming is instructions or code stored on the machine-readable storage medium and executable by the processor to perform the designated function.

[0019] Security indicator engine 121 may identify a security indicator that is originated from a source entity. The security indicator may comprise at least one observable. A “security indicator,” as used herein, may refer to a detection guidance for a security threat and/or vulnerability. In other words, the security indicator may specify what to detect or look for (e.g., an observable) and/or what it means if detected. For example, the security indicator may specify a certain Internet Protocol (IP) address to look for in the network traffic. The security indicator may include the information that the detection of that IP address in the network traffic can indicate a certain malicious security threat such as a Trojan virus. An “observable,” as used herein, may refer to an event pertinent to the operation of computers and networks (e.g., an event occurring in network, servers, applications, databases, and/or various components of any computer system). Examples of an observable may include but not be limited to: an IP address, a domain name, an e-mail address, Uniform Resource Locator (URL), and a software file hash. A security indicator may comprise a single observable (e.g., “a new file is created by an executable”) or a plurality of observables (e.g., “a new file is created by an executable and "the executable connects to domain X"”).

[0020] A security indicator may be created by and/or originated from at least one of a plurality of source entities. For example, the plurality of source entities may include a user (e.g., analysts and/or community members of the security information sharing platform). A security indicator may be manually created and/or added to the security information sharing platform by the user. In another example, the plurality of source entities may include a threat intelligence provider that provides threat intelligence feeds and/or any other participating organizations. A security indicator that is found in the intelligence feeds and/or information from other participating organizations, for example, may be automatically created and/or added to the security information sharing platform. There exist a number of providers of threat intelligence feeds. The threat intelligence feeds may be provided by independent third parties such as
security service providers. These providers and/or sources may supply the threat intelligence feeds that provide information about threats the providers have identified. Most threat intelligence feeds, for example, include lists of domain names, IP addresses, and URLs that various providers have classified as malicious or at least suspicious according to different methods and criteria. In another example, the plurality of source entities may include a third-party researcher or analyst.

[0021] In another example, a source entity may include an external resource (e.g., that is external to the security information sharing platform) such as web resources (e.g., a web forum, Internal Relay Chat (IRC) channel, social media, a publisher of articles). In this case, note that a source entity may be an individual creator/author of the content that is exchanged via these web resources (e.g., an author of a message posted on the message forum, an author of a social media post, an author of an article, etc.). On the other hand, a source entity may represent the external resource itself that supplies or otherwise provides the content is created by individual creators/authors.

[0022] In some implementations, the security information sharing platform may obtain and/or store (e.g., in a data storage 129) information related to the security indicator. Examples of the information related to the security indicator may include but are not limited to: an indicator score associated with the security indicator (e.g., as discussed herein with respect to indicator score engine 125), information related to a source entity of the indicator (e.g., identification of the source entity, level of source reliability associated with the source entity as discussed herein with respect to source reliability engine 125, level of source authenticity associated with the source entity as discussed herein with respect to source authenticity engine 124, etc.), a level of severity (e.g., the level of severity that the indicator may pose) associated with the security indicator (e.g., as discussed herein with respect to security indicator engine 121), and information related to an observable in the security indicator (e.g., information related to a source entity that provided the observable, sightings of the observable as discussed herein with respect to sighting engine 122, etc.), a threat actor for the security indicator (e.g., attacker behind the threat indicated in the security indicator), a domain name, a timestamp,
a campaign, a technique/tactic/procedure (TTP), and a group that the security indicator belongs to (e.g., an organization, an industry sector, a community of the security information sharing platform, etc.).

Sighting engine 122 may obtain, from a source entity, a sighting of an observable. The sighting of the observable may indicate that the observable has been observed by the source entity. For example, the source entity (e.g., the examples of the source entity are discussed herein with respect to security indicator engine 121) may detect a certain IP address (e.g., the observable) in its network traffic, and add the observable to the security information sharing platform. This addition of the observable may be considered as a single sighting of the observable. In some instances, when two individuals working for the same organization add the same observable to the platform, sighting engine 122 may treat these additions as a single sighting of the observable or as two separate sightings of the observable. In another example, when the IP address (e.g., the observable) is found in the threat intelligence feeds provided by a particular threat intelligence provider, this observable may be added to the security information sharing platform as a single sighting of this observable. When two different set of threat intelligence feeds provided by two different providers include the same observable, the observable may be added as two sightings of the observable.

Sighting engine 122 may determine a number (e.g., count) of sightings of the observable. For example, sighting engine 122 may obtain, from a first source entity, a first sighting of the observable that indicates that the observable has been observed by the first source entity. Sighting engine 122 may obtain, from a second source entity, a second sighting of the observable that indicates that the observable has been observed by the second source entity. In this case, the number of sightings of this observable may be 2. Note that the same observable may be associated with more than one security indicator. For example, a certain IP address may be part of a first security indicator (e.g., a finding of this IP address indicates a Trojan virus) as well as a second security indicator (e.g., a finding of this IP address visiting a particular URL indicates a Trojan virus). As such, a single sighting of the observable may be counted as one
sighting for each of the first security indicator and the second security indicator. Therefore, a single sighting of the observable associated with more than one security indicator can influence the respective indicator scores associated with those security indicators. In some implementations, sighting engine 122 may determine a normalized value of the number of sightings using a normalization algorithm. Any normalization algorithm known in the art may be used to determine the normalized value.

Source reliability engine 123 may identify and/or determine a reliability level of a particular source entity based on various parameters including, but not being limited to: (1) security events, (2) sightings of the observable, (3) a set of user feedback information that is submitted for the security indicator by users of the security information sharing platform, (4) a set of user feedback information and/or other information that is collected from external resources that are external to the security information sharing platform, and (5) a default or hard-coded reliability level. Each of the above parameters for determining the source reliability level is discussed in detail below.

(1) Security events: A "security event," as used herein, may include at least one security indicator and/or observable that are related to the same security event, and/or other information that may be relevant to that event (e.g., information related to a security indicator, user comments, etc.). For example, a user may create a new security event in the security information sharing platform after noticing an unusual activity in the network. The user and/or other users that are authorized to access the security event may create and/or submit a security indicator to the security event. The user and/or other users that are authorized to access the security event may identify a security indicator that has been provided by another source entity to include it in the security event. If a large number of security events include security indicators or other data items (e.g., threat actor, industry sector, etc.) that originate from a particular source entity, this could mean that the particular source entity has a track record of providing reliable information. As such, source reliability engine 123 may determine the reliability level of the particular source entity based on the number of security events that include
security indicators and/or other data items that originated from that particular source entity.

[0027] (2) Sightings of the observable: The sightings of the observable may be used to determine the reliability level of the source entity that provided the observable and/or security indicator having that observable. For example, based on the number of sightings of the observable (e.g., that may be determined as discussed herein with respect to sighting engine 122), the source reliability may be increased or decreased. In some cases, a high number of sightings may indicate that the source entity provided accurate information to the platform, resulting in a higher source reliability for the source entity. In other cases, a high number of sightings of inaccurate information (e.g., a popular website that is benign) may result in a lower source reliability for the source entity.

[0028] (3) A set of user feedback information that is submitted for the security indicator by users of the security information sharing platform: Users of the security information sharing platform may provide user feedback on a particular security indicator (and/or on a particular source entity, in some instances). The user feedback may include a comment, a rating, a vote, a selection from a list of options, etc. For example, a vote may indicate whether the security indicator is accurate. Source reliability engine 123 may obtain a set of votes associated with the particular security indicator from the users of the platform, and/or determine a reliability level of a source entity from which the particular security indicator originated based on the set of votes (e.g., the number of positive, neutral, and/or negative votes made to the security indicator).

[0029] (4) A set of user feedback information and/or other information that is collected from external resources that are external to the security information sharing platform: In some situations, a set of user feedback information may be collected from any of the external resources. In one example, source reliability engine 123 may evaluate statements and/or comments from the external resources (e.g., a web forum, social media, IRC channel, publisher, etc.) regarding the utility of the source-entity provided information (e.g., security indicators provided by a particular source entity) in resolving their security incidents or how helpful they found the provided information to be for detection purposes. Positive
comments regarding the source entity and/or the source-entity provided information may, for example, positively influence the reliability level of that source entity. In another example, a survey may be provided to external entities to collect a set of user feedback information on a particular security indicator and/or a particular source entity. Source reliability engine 123 may periodically collect the user feedback information from the external resources.

[0030] In some implementations, source reliability engine 123 may determine a reliability level of a particular source entity based on a comparison between (3) the set of user feedback information that is submitted for the security indicator (e.g., that originated from the particular source entity) by users of the security information sharing platform and (4) the set of user feedback information that is collected from the external resources regarding the security indicator. For example, if the result of the comparison indicates a discrepancy above a certain threshold value, the reliability level for the particular source entity should be lowered. On the other hand, if the result of the comparison indicates a similarity above a certain threshold, the reliability level for the source entity could be increased.

[0031] In some implementations, an external resource could represent a source entity itself, and source reliability engine 123 may determine a reliability level of the external resource as a source entity. For example, there may be an external resource that publishes or otherwise provides various articles. The various articles may be written by different individual authors. If an article contains content (e.g., content about a threat actor) that is related to a security indicator in the platform, that external resource may be given a higher reliability level.

[0032] (5) A default or hard-coded reliability level: A default reliability level may be set by a user and/or by system 110. A default reliability level may be set for an individual source entity and/or a group of source entities. If the reliability level for a particular source entity is unknown or otherwise cannot be determined, the default reliability level may be used for the particular source entity. In some instances, the reliability level may be hard-coded, meaning the hard-coded reliability level would overwrite the reliability level that is determined based on other parameters described above.
Source authenticity engine 124 may determine an authenticity level of a particular source entity based on a type of the source entity. The type of the source entity may comprise a non-trusted source type or a trusted source type. For example, a source entity such as a government entity (e.g., Federal Bureau of Investigation (FBI)) may be given a high authenticity level whereas an email or a social media message from a non-trusted or non-verified source should be given a low authenticity level. Generally, threat intelligence feed providers that have been verified are given a high authenticity level. External resources, in particular web resources as discussed above, may be given a low authenticity level because they usually apply a low level of scrutiny to the content therein.

Indicator score engine 125 may determine an indicator score associated with the security indicator (e.g., that originated from a particular source entity) based on various parameters including, but not being limited to: a severity level associated with the security indicator, the reliability level of the particular source entity (e.g., as discussed herein with respect to source reliability engine 123), and the authenticity level of the particular source entity (e.g., as discussed herein with respect to source authenticity engine 124). In some implementations, each of the parameters may be scaled by a corresponding weight. The weight may represent the weight or influence the particular parameter has on the indicator score. For example, the weight value may be any value from 0 to 100. The total sum of all weights of the parameters being used to determine the indicator score can be 100 in some situations, but is not necessarily 100.

In some implementations, a recommendation and/or a recommended action may be generated or otherwise provided based on the indicator score (e.g., as discussed herein with respect to indicator score engine 125) of the security indicator. For example, if the indicator score is below a first threshold value, the indicator can be continued to be monitored without any further action. If the indicator score is above the first threshold value but below a second threshold value, the recommendation may be generated to inform at least one user to perform a further investigation on the security indicator. If the indicator score is above a third threshold value, the indicator may be considered to be malicious and/or accurate that could pose an actual security threat. In this case, any event
that matches this security indicator may be blocked from accessing certain resources.

[0036] In performing their respective functions, engines 121-125 may access data storage 129 and/or other suitable database(s). Data storage 129 may represent any memory accessible to source entities system 110 that can be used to store and retrieve data. Data storage 129 and/or other database may comprise random access memory (RAM), read-only memory (ROM), electrically-erasable programmable read-only memory (EEPROM), cache memory, floppy disks, hard disks, optical disks, tapes, solid state drives, flash drives, portable compact disks, and/or other storage media for storing computer-executable instructions and/or data. Source entities system 110 may access data storage 129 locally or remotely via network 50 or other networks.

[0037] Data storage 129 may include a database to organize and store data. The database may reside in a single or multiple physical device(s) and in a single or multiple physical location(s). The database may store a plurality of types of data and/or files and associated data or file description, administrative information, or any other data.

[0038] FIG. 2 is a block diagram depicting an example source entities system 210. Source entities system 210 may comprise a security indicator engine 221, a source reliability engine 223, an indicator score engine 225, and/or other engines. Engines 221, 223, and 225 represent engines 121, 123, and 125, respectively.

[0039] FIG. 3 is a block diagram depicting an example machine-readable storage medium 310 comprising instructions executable by a processor for source entities of security indicators.

[0040] In the foregoing discussion, engines 121-125 were described as combinations of hardware and programming. Engines 121-125 may be implemented in a number of fashions. Referring to FIG. 3, the programming may be processor executable instructions 321-325 stored on a machine-readable storage medium 310 and the hardware may include a processor 311 for executing those instructions. Thus, machine-readable storage medium 310 can be said to store program instructions or code that when executed by processor 311 implements source entities system 110 of FIG. 1.
[0041] In FIG. 3, the executable program instructions in machine-readable storage medium 310 are depicted as security indicator instructions 321, sighting instructions 322, source reliability instructions 323, source authenticity instructions 324, indicator score instructions 325. Instructions 321-325 represent program instructions that, when executed, cause processor 311 to implement engines 121-125, respectively.

[0042] FIG. 4 is a block diagram depicting an example machine-readable storage medium 410 comprising instructions executable by a processor for source entities of security indicators.

[0043] In the foregoing discussion, engines 121-125 were described as combinations of hardware and programming. Engines 121-125 may be implemented in a number of fashions. Referring to FIG. 4, the programming may be processor executable instructions 421 and 423-425 stored on a machine-readable storage medium 410 and the hardware may include a processor 411 for executing those instructions. Thus, machine-readable storage medium 410 can be said to store program instructions or code that when executed by processor 411 implements source entities system 110 of FIG. 1.

[0044] In FIG. 4, the executable program instructions in machine-readable storage medium 410 are depicted as security indicator instructions 421, source reliability instructions 423, source authenticity instructions 424, and indicator score instructions 425. Instructions 421 and 423-425 represent program instructions that, when executed, cause processor 411 to implement engines 121 and 123-125, respectively.

[0045] Machine-readable storage medium 310 (or machine-readable storage medium 410) may be any electronic, magnetic, optical, or other physical storage device that contains or stores executable instructions. In some implementations, machine-readable storage medium 310 (or machine-readable storage medium 410) may be a non-transitory storage medium, where the term "non-transitory" does not encompass transitory propagating signals. Machine-readable storage medium 310 (or machine-readable storage medium 410) may be implemented in a single device or distributed across devices. Likewise, processor 311 (or processor 411) may represent any number of processors capable of executing
instructions stored by machine-readable storage medium 310 (or machine-readable storage medium 410). Processor 311 (or processor 411) may be integrated in a single device or distributed across devices. Further, machine-readable storage medium 310 (or machine-readable storage medium 410) may be fully or partially integrated in the same device as processor 311 (or processor 411), or it may be separate but accessible to that device and processor 311 (or processor 411).

In one example, the program instructions may be part of an installation package that when installed can be executed by processor 311 (or processor 411) to implement source entities system 110. In this case, machine-readable storage medium 310 (or machine-readable storage medium 410) may be a portable medium such as a floppy disk, CD, DVD, or flash drive or a memory maintained by a server from which the installation package can be downloaded and installed. In another example, the program instructions may be part of an application or applications already installed. Here, machine-readable storage medium 310 (or machine-readable storage medium 410) may include a hard disk, optical disk, tapes, solid state drives, RAM, ROM, EEPROM, or the like.

Processor 311 may be at least one central processing unit (CPU), microprocessor, and/or other hardware device suitable for retrieval and execution of instructions stored in machine-readable storage medium 310. Processor 311 may fetch, decode, and execute program instructions 321-325, and/or other instructions. As an alternative or in addition to retrieving and executing instructions, processor 311 may include at least one electronic circuit comprising a number of electronic components for performing the functionality of at least one of instructions 321-325, and/or other instructions.

Processor 411 may be at least one central processing unit (CPU), microprocessor, and/or other hardware device suitable for retrieval and execution of instructions stored in machine-readable storage medium 410. Processor 411 may fetch, decode, and execute program instructions 421 and 423-425, and/or other instructions. As an alternative or in addition to retrieving and executing instructions, processor 411 may include at least one electronic circuit comprising a
number of electronic components for performing the functionality of at least one of
instructions 421 and 423-425, and/or other instructions.

[0049] FIG. 5 is a flow diagram depicting an example method 500 for
determining reliability levels of source entities of security indicators. The various
processing blocks and/or data flows depicted in FIG. 5 (and in the other drawing
figures such as FIG. 6) are described in greater detail herein. The described
processing blocks may be accomplished using some or all of the system
components described in detail above and, in some implementations, various
processing blocks may be performed in different sequences and various
processing blocks may be omitted. Additional processing blocks may be
performed along with some or all of the processing blocks shown in the depicted
flow diagrams. Some processing blocks may be performed simultaneously.
Accordingly, method 500 as illustrated (and described in greater detail below) is
meant be an example and, as such, should not be viewed as limiting. Method 500
may be implemented in the form of executable instructions stored on a machine-
readable storage medium, such as storage medium 310, and/or in the form of
electronic circuitry.

[0050] In block 521, method 500 may include identifying, in a security
information sharing platform, a security indicator that is originated from a source
entity, the security indicator comprising an observable. Referring back to FIG. 1,
security indicator engine 121 may be responsible for implementing block 521.

[0051] In block 522, method 500 may include identifying, in the security
information sharing platform, security events that include information related to the
security indicator. Referring back to FIG. 1, source reliability engine 123 may be
responsible for implementing block 522.

[0052] In block 523, method 500 may include determining a reliability level of
the source entity based on at least one of: the security events, sightings of the
observable, or a set of user feedback information that is submitted for the security
indicator by users of the security information sharing platform. Referring back to
FIG. 1, source reliability engine 123 may be responsible for implementing block
523.
FIG. 6 is a flow diagram depicting an example method 600 for determining reliability and authenticity levels of source entities of security indicators. Method 600 as illustrated (and described in greater detail below) is meant to be an example and, as such, should not be viewed as limiting. Method 600 may be implemented in the form of executable instructions stored on a machine-readable storage medium, such as storage medium 310, and/or in the form of electronic circuitry.

In block 621, method 600 may include identifying, in a security information sharing platform, a security indicator that is originated from a source entity, the security indicator comprising an observable. Referring back to FIG. 1, security indicator engine 121 may be responsible for implementing block 621.

In block 622, method 600 may include identifying, in the security information sharing platform, security events that include information related to the security indicator. Referring back to FIG. 1, source reliability engine 123 may be responsible for implementing block 622.

In block 623, method 600 may include determining a reliability level of the source entity based on at least one of: the security events, sightings of the observable, or a set of user feedback information that is submitted for the security indicator by users of the security information sharing platform. Referring back to FIG. 1, source reliability engine 123 may be responsible for implementing block 623.

In block 624, method 600 may include determining an authenticity level of the source entity based on a type of the source entity, wherein the type of the source entity comprises: a non-trusted source type or a trusted source type. Referring back to FIG. 1, source authenticity engine 124 may be responsible for implementing block 624.

In block 625, method 600 may include determining an indicator score associated the security indicator based on at least one of: a severity level associated with the security indicator, the reliability level of the source entity, or the authenticity level of the source entity. Referring back to FIG. 1, indicator score engine 125 may be responsible for implementing block 625.
The foregoing disclosure describes a number of example implementations for source entities of security indicators. The disclosed examples may include systems, devices, computer-readable storage media, and methods for determining reliability and/or authenticity levels of source entities of security indicators. For purposes of explanation, certain examples are described with reference to the components illustrated in FIGS. 1-4. The functionality of the illustrated components may overlap, however, and may be present in a fewer or greater number of elements and components.

Further, all or part of the functionality of illustrated elements may co-exist or be distributed among several geographically dispersed locations. Moreover, the disclosed examples may be implemented in various environments and are not limited to the illustrated examples. Further, the sequence of operations described in connection with FIGS. 5-6 are examples and are not intended to be limiting. Additional or fewer operations or combinations of operations may be used or may vary without departing from the scope of the disclosed examples. Furthermore, implementations consistent with the disclosed examples need not perform the sequence of operations in any particular order. Thus, the present disclosure merely sets forth possible examples of implementations, and many variations and modifications may be made to the described examples. All such modifications and variations are intended to be included within the scope of this disclosure and protected by the following claims.
CLAIMS

1. A method for source entities of security indicators, the method comprising:
   identifying, in a security information sharing platform, a security indicator that is originated from a first source entity, the security indicator comprising an observable;
   identifying, in the security information sharing platform, security events that include information related to the security indicator; and
   determining a reliability level of the first source entity based on at least one of: the security events, sightings of the observable, or a first set of user feedback information that is submitted for the security indicator by users of the security information sharing platform.

2. The method of claim 1, further comprising:
   determining an authenticity level of the first source entity based on a type of the first source entity, wherein the type of the first source entity comprises: a non-trusted source type or a trusted source type.

3. The method of claim 2, further comprising:
   determining an indicator score associated with the security indicator based on at least one of: a severity level associated with the security indicator, the reliability level of the first source entity, or the authenticity level of the first source entity.

4. The method of claim 1, further comprising:
   identifying, in an external resource that is external to the security information sharing platform, a second set of user feedback information about the security indicator or the first source entity; and
   determining the reliability level of the first source entity based on the second set of user feedback information.

5. The method of claim 1, further comprising:
providing a survey to collect a second set of user feedback information on the security indicator or the first source entity; and determining the reliability level of the first source entity based on the second set of user feedback.

6. The method of claim 1, further comprising:
obtaining an article via a second source entity;
determining whether the article includes information related to the security indicator; and
determining the reliability level of the second source entity based on the determination of whether the article includes the information related to the security indicator.

7. The method of claim 6, wherein the information related to the security indicator comprises at least one of: a threat actor, a campaign, a technique/tactic/procedure (TTP), an organization, an industry sector, a community, a domain name, a timestamp, or a level of severity of the first security indicator.

8. A non-transitory machine-readable storage medium comprising instructions executable by a processor of a computing device for source entities of security indicators, the machine-readable storage medium comprising:
instructions to identify, in a security information sharing platform, a first security indicator that is originated from a first source entity, the first security indicator comprising a first observable;
instructions to determine a reliability level of the first source entity based on at least one of: a first set of user feedback information that is submitted for the first security indicator by users of the security information sharing platform, or a second set of user feedback information that is collected from external resources that are external to the security information sharing platform;
instructions to determine an authenticity level of the first source entity based on a type of the first source entity; and
instructions to determine an indicator score associated with the first
security indicator based on at least one of: a severity level associated with the
first security indicator, the reliability level of the first source entity, or the
authenticity level of the first source entity.

9. The non-transitory machine-readable storage medium of claim 8, further
comprising:
   instructions to identify, in the security information sharing platform, a
second security indicator that is originated from a second source entity, the
second security indicator comprising a second observable;
   instructions to determine a reliability level of the second source entity
based on at least one of: a third set of user feedback information that is
submitted for the second security indicator by the users of the security
information sharing platform, or a fourth set of user feedback information that is
collected from the external resources;
   instructions to determine an authenticity level of the second source entity
based on a type of the second source entity; and
   instructions to determine an indicator score associated with the second
security indicator based on at least one of: a severity level associated with the
second security indicator, the reliability level of the second source entity, or the
authenticity level of the second source entity.

10. The non-transitory machine-readable storage medium of claim 8, further
comprising:
   instructions to determine a number of security events that are created in
the security information sharing platform, wherein the security events include
the first security indicator; and
   instructions to determine the reliability level of the first source entity
based on the number of security events.

11. The non-transitory machine-readable storage medium of claim 8, further
comprising:
instructions to obtain, from a second source entity, a first sighting of the first observable, the first sighting of the first observable indicating that the first observable has been observed by the second source entity;
instructions to obtain, from a third source entity, a second sighting of the first observable, the second sighting of the first observable indicating that the first observable has been observed by the third source entity;
instructions to determine a number of sightings of the first observable, the sightings of the first observable including the first and second sightings of the first observable; and
instructions to determine the reliability level of the first source entity based on the number of sightings.

12. The non-transitory machine-readable storage medium of claim 8, further comprising:
   comparing the first set of user feedback information and the second set of user feedback information; and
   adjusting the reliability level of the first source entity based on the comparison.

13. A system for source entities of security indicators comprising:
a processor that:
   identifies, in a security information sharing platform, a security indicator that is originated from a source entity, the security indicator comprising an observable;
determines a reliability level of the source entity based on at least one of: sightings of the observable, a first set of user feedback information that is submitted for the security indicator by users of the security information sharing platform, or a second set of user feedback information that is collected from an external resource that is external to the security information sharing platform; and
determines an indicator score associated the security indicator based on a severity level associated with the security indicator and the reliability level of the source entity.

14. The system of claim 13, the processor that:
   determines an authenticity level of the source entity based on a type of the source entity; and
   determines the indicator score associated with the security indicator based on the severity level associated with the security indicator and the reliability and authenticity levels of the source entity.

15. The system of claim 13, the processor that:
   obtains a set of votes associated with the security indicator from the users of the security information sharing platform, individual votes of the set of votes indicating whether the security indicator is accurate; and
   including the set of votes in the first set of user feedback information.
FIG. 1
FIG. 2
FIG. 3

310 MACHINE-READABLE STORAGE MEDIUM

321 SECURITY INDICATOR INSTRUCTIONS

322 SIGHTING INSTRUCTIONS

323 SOURCE RELIABILITY INSTRUCTIONS

324 SOURCE AUTHENTICITY INSTRUCTIONS

325 INDICATOR SCORE INSTRUCTIONS

311 PROCESSOR

FIG. 4

410 MACHINE-READABLE STORAGE MEDIUM

421 SECURITY INDICATOR INSTRUCTIONS

423 SOURCE RELIABILITY INSTRUCTIONS

424 SOURCE AUTHENTICITY INSTRUCTIONS

425 INDICATOR SCORE INSTRUCTIONS

411 PROCESSOR
IDENTIFYING, IN A SECURITY INFORMATION SHARING PLATFORM, A SECURITY INDICATOR THAT IS ORIGINATED FROM A SOURCE ENTITY, THE SECURITY INDICATOR COMPRISING AN OBSERVABLE

IDENTIFYING, IN THE SECURITY INFORMATION SHARING PLATFORM, SECURITY EVENTS THAT INCLUDE INFORMATION RELATED TO THE SECURITY INDICATOR


FIG. 5
IDENTIFYING, IN A SECURITY INFORMATION SHARING PLATFORM, A SECURITY INDICATOR THAT IS ORIGINATED FROM A SOURCE ENTITY, THE SECURITY INDICATOR COMPRISING AN OBSERVABLE

IDENTIFYING, IN THE SECURITY INFORMATION SHARING PLATFORM, SECURITY EVENTS THAT INCLUDE INFORMATION RELATED TO THE SECURITY INDICATOR


FIG. 6
A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i, H04L 12/22(2006.01)i

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)

H04L 29/06; G06F 15/16; G06Q 10/06; H04L 9/00; H04L 12/22

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: security, sharing, platform, event, reliability, authenticity, security, level, indicator, score, feedback

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>KR 10-1505079 Bl (EVOLCANO INC CO., LTD. et a l.) 24 March 2015 See paragraphs [0036] ; [0058] ; and figure 1.</td>
<td>1-15</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C.

See patent family annex.

* 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

Date of the actual completion of the international search

26 October 2016 (26. 10. 2016)

Date of mailing of the international search report

02 November 2016 (02.11.2016)

Name and mailing address of the ISA/KR

International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer

KIM, Seong Woo

Telephone No. +82-42-481-3348

Form PCT/ISA/210 (second sheet) (January 2015)
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>EP 1491022 Al</td>
<td>29/12/2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GB 2422931 A</td>
<td>09/08/2006</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2003-0188194 Al</td>
<td>02/10/2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>wo 03-084182 Al</td>
<td>09/10/2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>wo 2005-033943 Al</td>
<td>14/04/2005</td>
</tr>
<tr>
<td></td>
<td></td>
<td>wo 2005-033943 Bl</td>
<td>26/05/2005</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2874320 Al</td>
<td>03/01/2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 2867810 Al</td>
<td>06/05/2015</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2015-524585 A</td>
<td>24/08/2015</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2014-007190 Al</td>
<td>02/01/2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 9292881 B2</td>
<td>22/03/2016</td>
</tr>
<tr>
<td></td>
<td></td>
<td>wo 2014-003900 Al</td>
<td>03/01/2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 105378790 A</td>
<td>02/03/2016</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 2973382 Al</td>
<td>20/01/2016</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 9300676 B2</td>
<td>29/03/2016</td>
</tr>
<tr>
<td></td>
<td></td>
<td>wo 2014-145431 Al</td>
<td>18/09/2014</td>
</tr>
<tr>
<td>kR 10-1505079 Bl</td>
<td>24/03/2015</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>