



(19) **United States**

(12) **Patent Application Publication**
Moen et al.

(10) **Pub. No.: US 2019/0140835 A1**

(43) **Pub. Date: May 9, 2019**

(54) **BLIND HASH COMPRESSION**

(52) **U.S. Cl.**

(71) Applicant: **Shape Security, Inc.**, Mountain View, CA (US)

CPC **H04L 9/3236** (2013.01); **H04L 2209/30** (2013.01); **H04L 9/3239** (2013.01); **G06F 21/577** (2013.01)

(72) Inventors: **Daniel G. Moen**, Sunnyvale, CA (US); **Bryan D. Hanks**, San Jose, CA (US)

(57) **ABSTRACT**

(73) Assignee: **Shape Security, Inc.**, Mountain View, CA (US)

Techniques are provided for blind hash compression, such as serving, from a computer server system and to a plurality of different computing devices remote from the computer server system, web code and code for reporting status of the computing devices; receiving from one or more of the computing devices, first data that indicates a parameter of the one or more computing devices, the first data in a compressed format; receiving from one or more others of the computing devices, second data that indicates the parameter of the one or more others of the computing devices, the second data in an uncompressed format; and compressing the second data and comparing the compressed second data to the first data to correlate the first data to the second data. The code for reporting status of the computing devices can include code for allowing the computing devices to determine whether to send the first or second data.

(21) Appl. No.: **16/236,566**

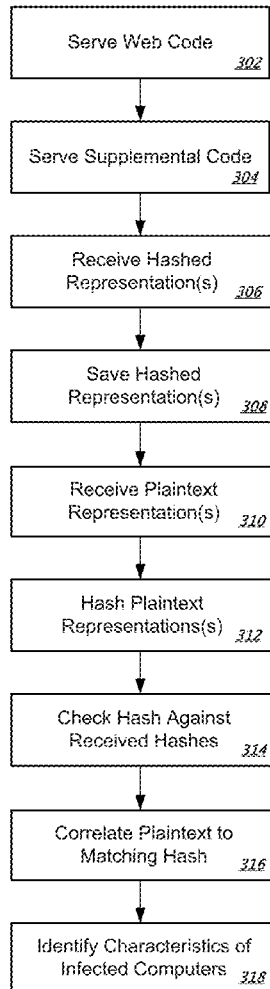
(22) Filed: **Dec. 30, 2018**

Related U.S. Application Data

(63) Continuation of application No. 14/160,107, filed on Jan. 21, 2014, now Pat. No. 9,225,729.

Publication Classification

(51) **Int. Cl.**
H04L 9/32 (2006.01)
G06F 21/57 (2006.01)



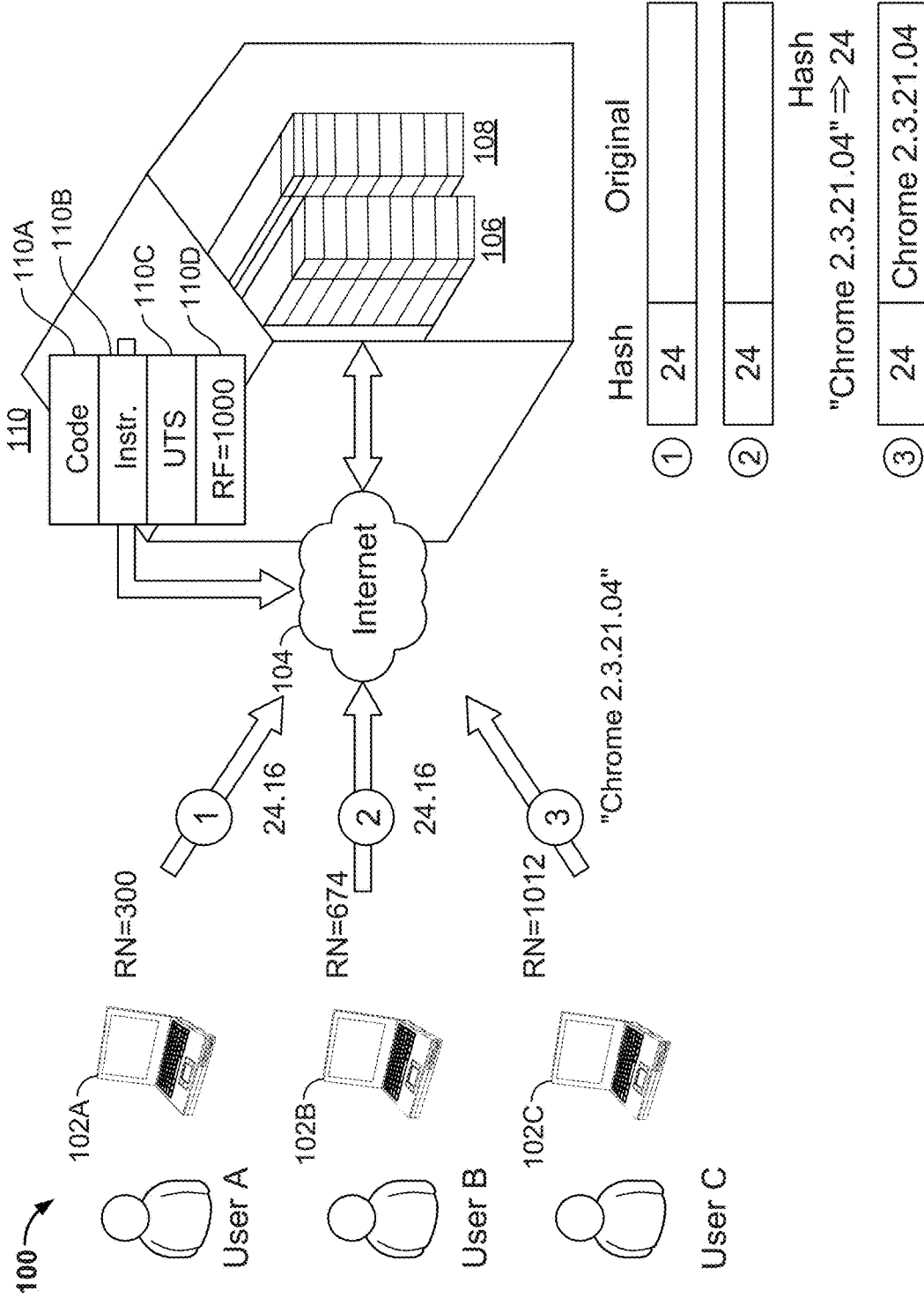


FIG. 1

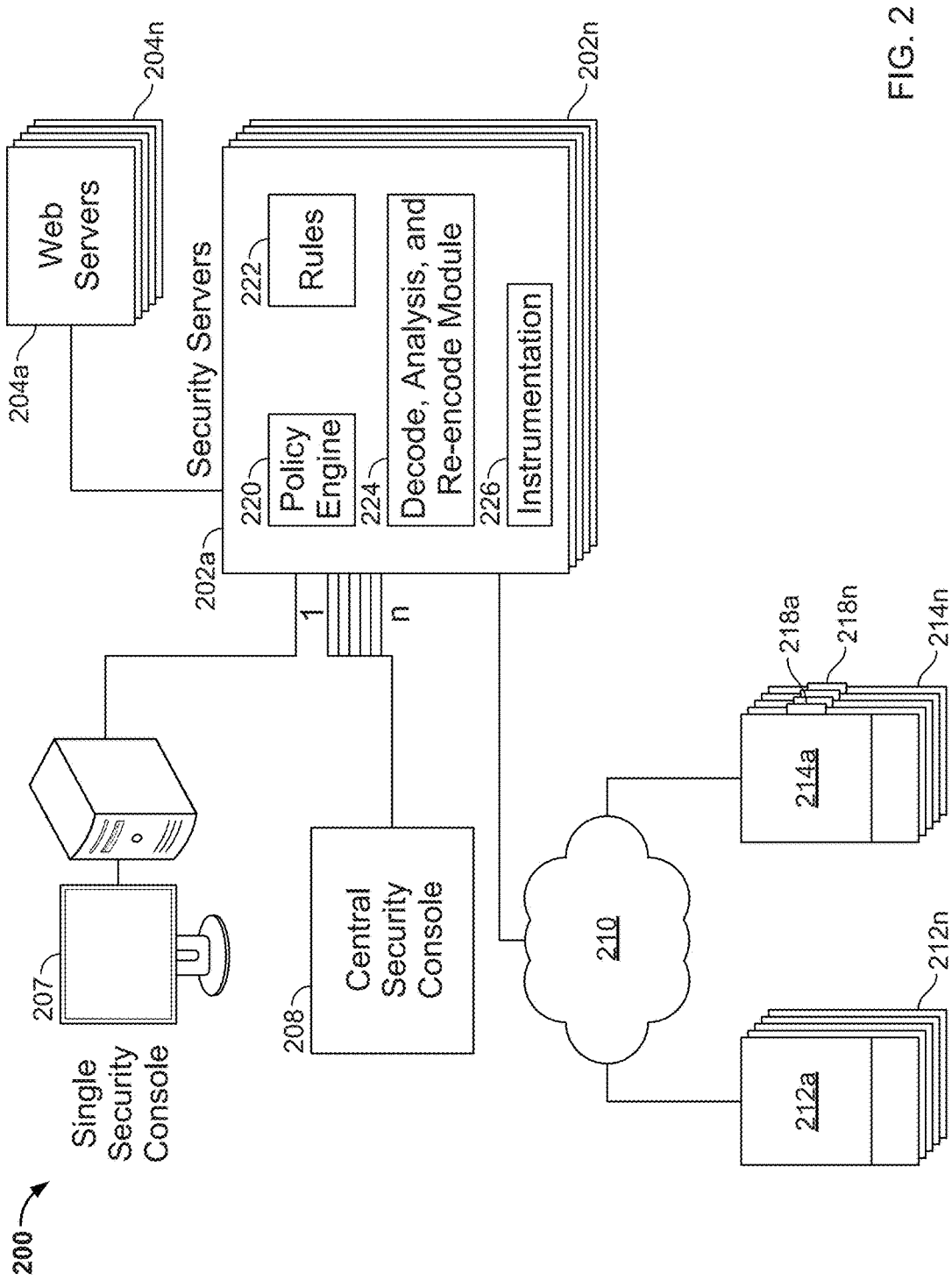


FIG. 2

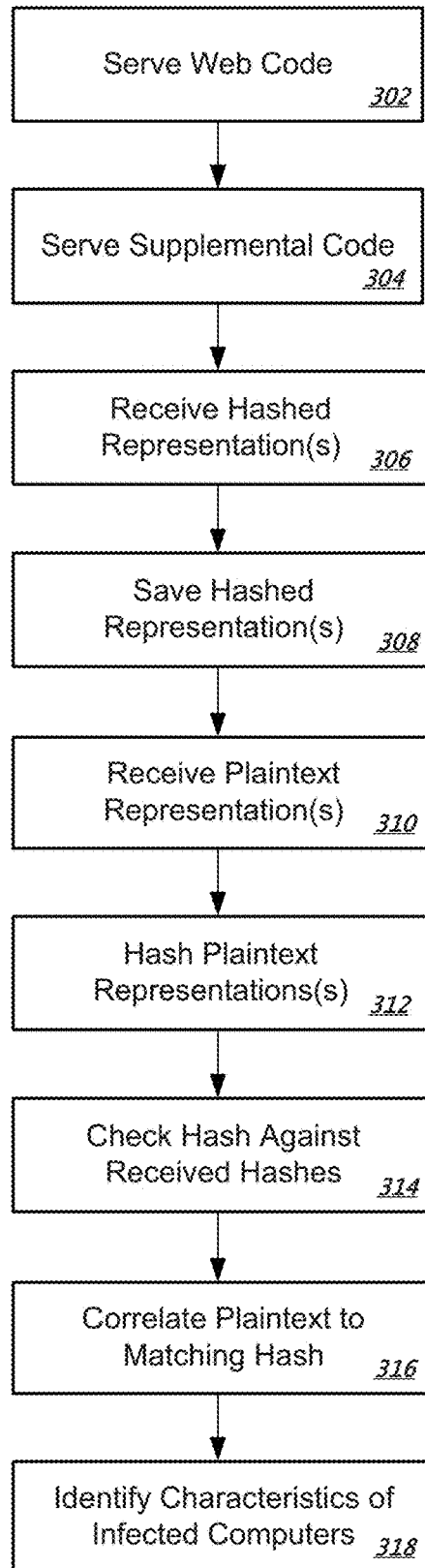


FIG. 3

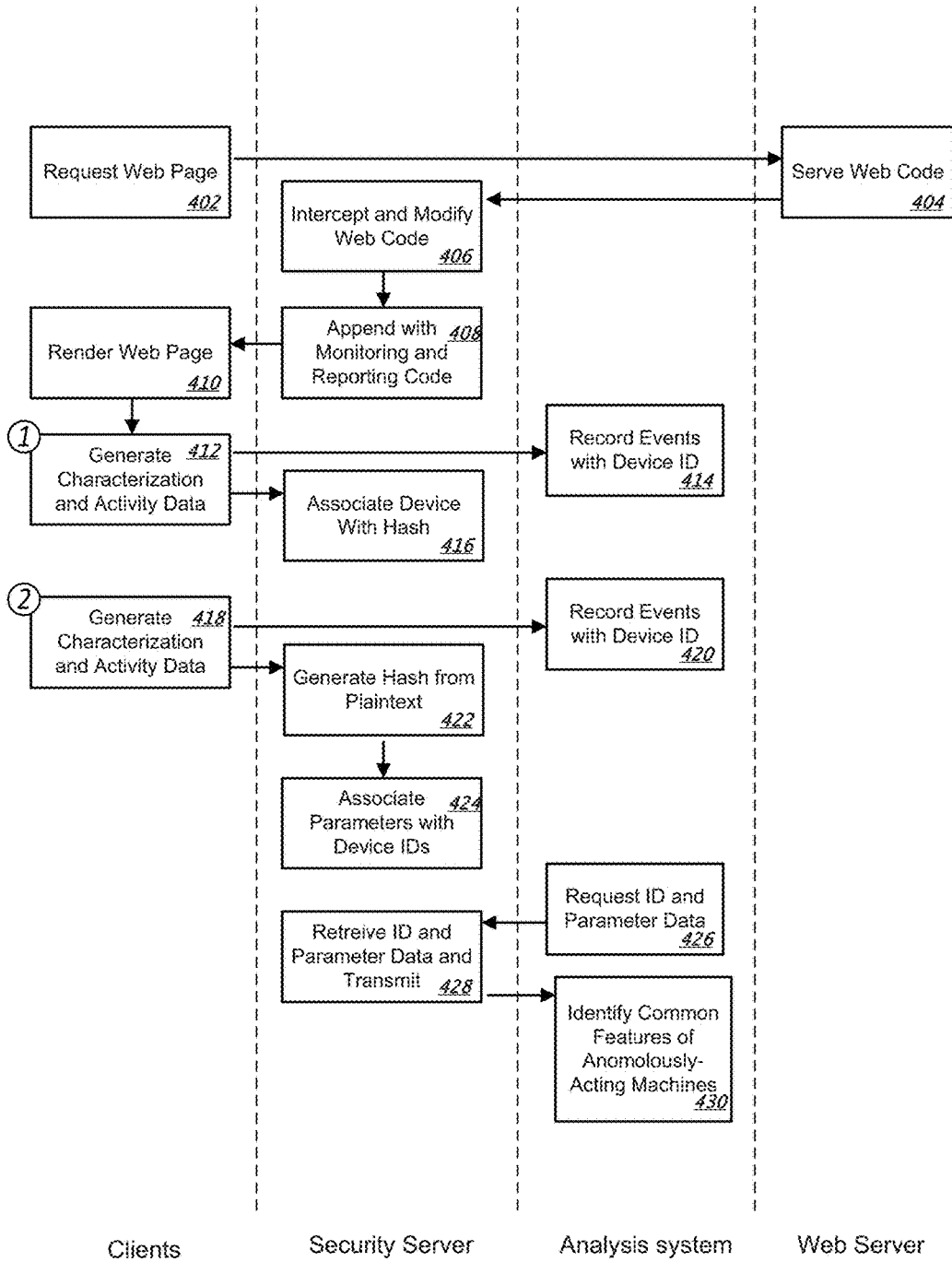


FIG. 4

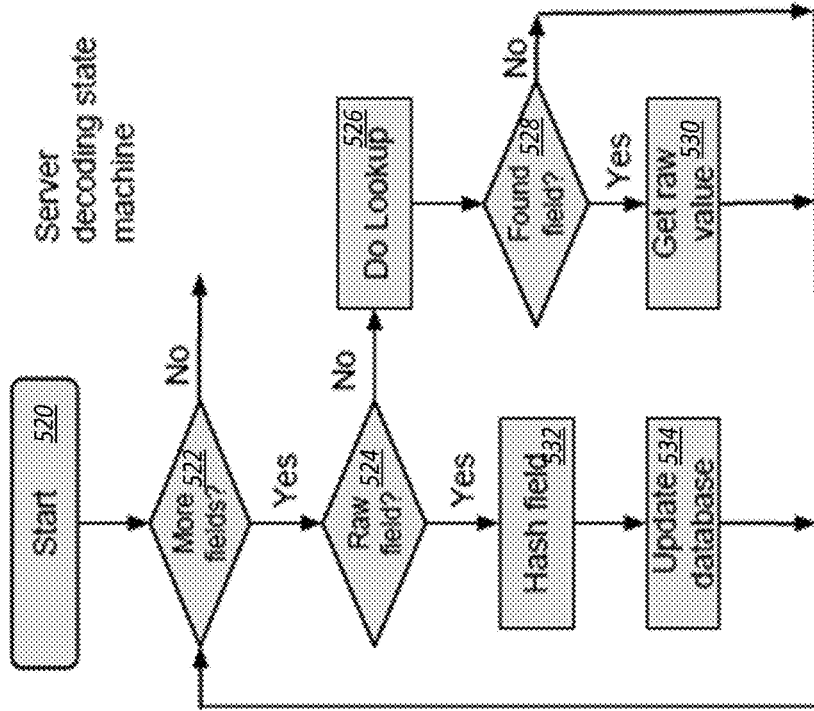


FIG. 5B

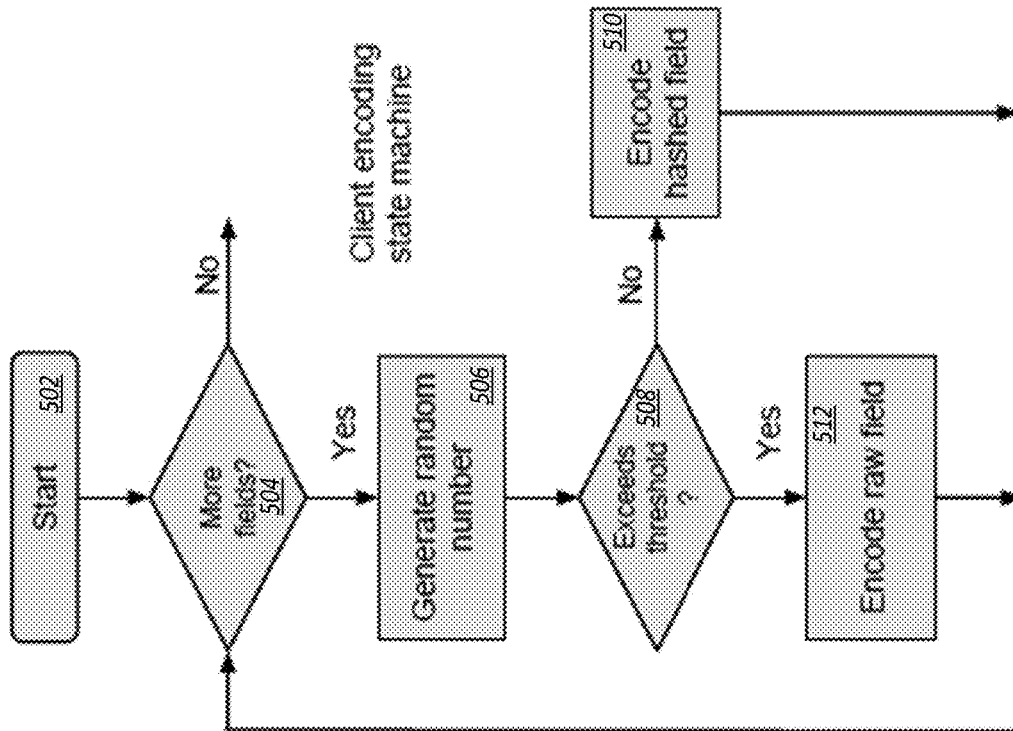


FIG. 5A

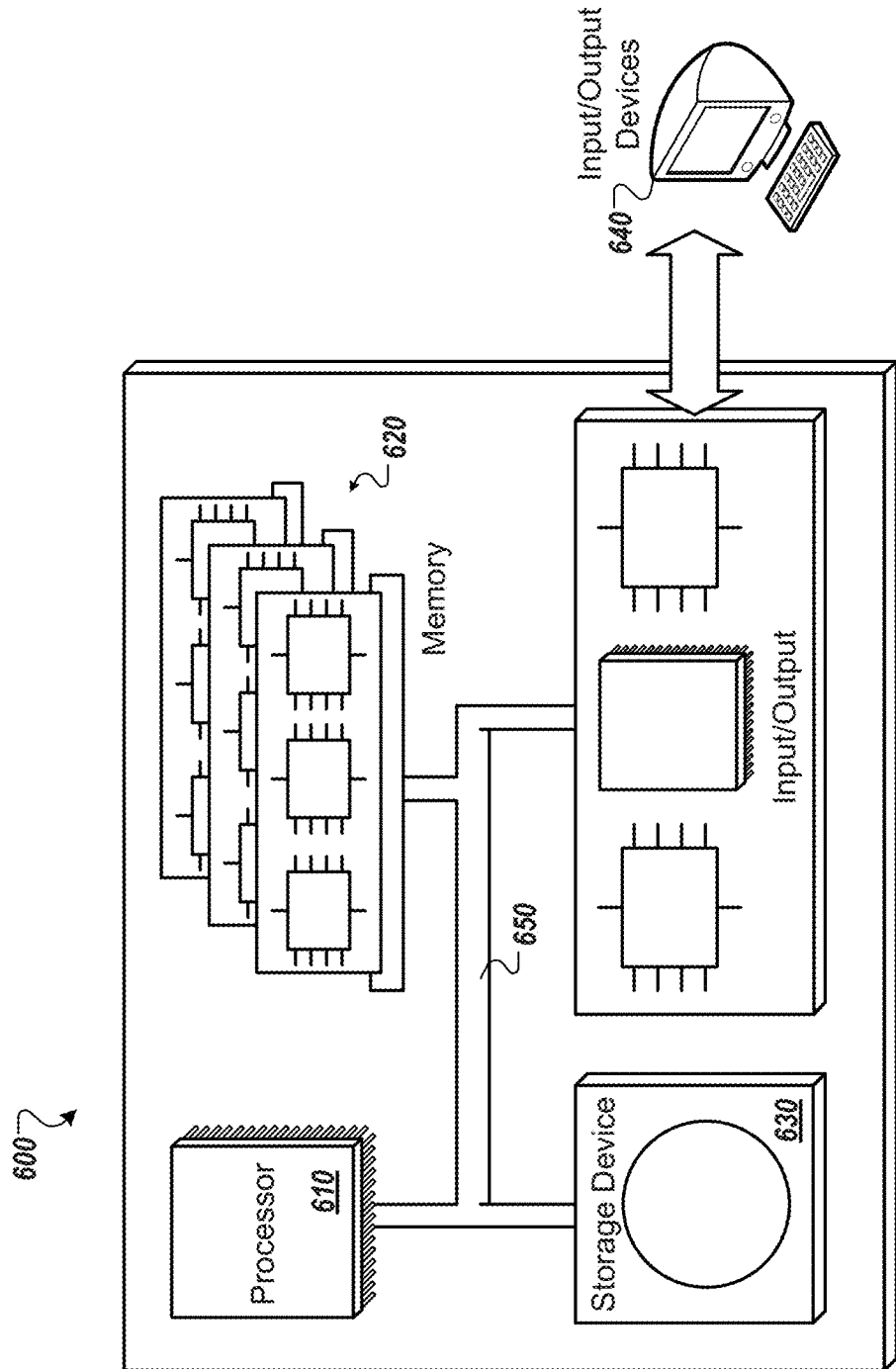


FIG. 6

BLIND HASH COMPRESSION

CROSS-REFERENCE TO RELATED APPLICATIONS; BENEFIT CLAIM

[0001] This application claims the benefit under 35 U.S.C. § 120 as a Continuation of U.S. patent application No. 14/980,231, filed on 2015-12-28, which is a Continuation of U.S. patent application No. 14/160m107, filed on 2014-1-21, the entire contents of which are hereby incorporated by reference as if fully set forth herein.

FIELD OF THE DISCLOSURE

[0002] This document generally relates to computer communications.

BACKGROUND

[0003] The approaches described in this section are approaches that could be pursued, but not necessarily approaches that have been previously conceived or pursued. Therefore, unless otherwise indicated, it should not be assumed that any of the approaches described in this section qualify as prior art merely by virtue of their inclusion in this section.

[0004] Web content, such as HTML or JavaScript for generating web pages, may contain application-like functionality that is interpreted and executed within a visitor's browser, or in a similar application. The general goal with HTML and other web technologies is to make them work, and work similarly, across many different platforms (e.g., Mac, PC, Linux, etc.).

[0005] To maximize the functionality of web content, it can be relevant for a system that serves the content to know the configurations of computers (whether desktop, smartphone, tablet, or other) that are being served the content. For example, particular knowledge can be obtained by identifying the type of browser that is rendering a web page, the operating system on which the browser is running, and plug ins that might also be operating on such computers. However, this additional supporting information must generally be sent from the various client computers to the server system, and such transmission adds overhead to the functioning of a browser presenting a web page or other application, which overhead is not directly responsible for improving operation of the page.

SUMMARY

[0006] This document describes systems and techniques by which various user computing devices (computers such as desktops, laptops, tablets, and smartphones) can submit information to a server system in a manner that lowers the bandwidth required for such reporting. Specifically, certain of the computing devices can send information in a lossy compressed format (e.g., as a hash of the original information), while others can send the same information in an uncompressing format (e.g., as the original plaintext).

[0007] The compressed format may be highly compressed, such as by a lossy one-way function so that the server system cannot immediately determine what original string a compressed submission is indicative of (e.g., via a hash function or other lossy compression function).

[0008] To determine what the compressed submissions represent, the server system compresses any received uncompressed submissions (or submitted with lossless com-

pression) using the same technique used by the client devices to perform their compression, at which point the server system knows the correlation between the uncompressed and compressed representations, and can then correlate any previously- or later-received compressed representations back to the original raw data. The percentage of the client computers reporting raw data may be much smaller than those reporting compressed data, so that the overall bandwidth of the system is substantially reduced. For example, each of the computing devices may determine whether it should submit a compressed representation of the data, or instead, an uncompressed representation by generating a random number (again, e.g., using standard JavaScript functions), and only send a particular format or representation if the generated number is above or below a predetermined number, as the case may be.

[0009] The server system may provide a biasing value to the computing devices when it serves web code so as to push the random number higher or lower, so as to affect the likelihood that any particular computing device will send uncompressed, raw data instead of compressed data. More frequent submission of uncompressed representations will allow a server system to more quickly identify the real meaning of data that newly arrives, e.g., when new features arrive on the computing devices (e.g., new plug ins are announced), but could cause higher bandwidth usage in a pool of computing devices. Thus, an operator of a server system may use the biasing value to match its desire for fast reaction versus its desire for lower bandwidth requirements.

[0010] To further minimize the amount of data transfer needed, the compression algorithm may be one that is available from public libraries, such as standard JavaScript hash algorithms. In this manner, the server system may automatically obtain plaintext representations of new data as it arrives in a pool of computers (e.g., all computers trying to access a particular retailer's web site), but may also determine how broadly such information has spread without having to send the potentially voluminous plaintext representation for very many of the computing devices.

[0011] Generally, hashing algorithms are selective enough that very few collisions will be seen between hashes (i.e., two different strings of text sent by computing devices will seldom generate the same hash value). When there are collisions, however, a server system will not be able to determine what is meant by such a compressed value when it arrives (it will be ambiguous as between the two or more source strings that generate the compressed value). Thus, the system just discussed may also include provisions for resolving such collisions. For example, a computing device may perform a secondary compression that uses a different algorithm than the primary compression, so that if the values of both compressions do not match across different submissions, then the source text for those different submissions is known to be different. Alternatively, or in addition, a length of the source string may also be submitted as to serve as yet another separate check on the source string.

[0012] In particular implementations of such techniques, the collected data may be configuration data for the computing devices, which may include, for example, the make and model of the computer, the make and version of the operating system and the web browser that is being used, the identity of active plug ins and other applications currently executing on the computing device in addition to the browser, among other things, such as installed fonts, screen

resolution, etc. Collected data may also include activity data that identifies actions that have been taken on the computer, including actions by third-party software that appears to be anomalous (e.g., attempts to interact with the revised web code in an invalid manner). Such data may be collected by one or more central server systems for diagnostics purposes, including for identifying the state of machines when a program throws an error, and for identifying common characteristics of computing devices that are exhibiting fraudulent or other anomalous behavior. For example, a criminal group may have a plug in or other software surreptitiously distributed to thousands of computers spread across the world to form a so-called bot net, and the server system discussed here may use reporting information from such computers to more quickly and accurately identify the presence of a new bot net that is emerging, and the behavior of that bot net (e.g., if common reports of malicious activity are coming from a particular operating system running a particular browser version).

[0013] Various implementations are described herein using hardware, software, firmware, or a combination of such components. In some implementations, a computer-implemented method can include serving, from a computer server system and to a plurality of different computing devices remote from the computer server system, web code and code for reporting parameters of the computing devices; receiving from different ones of the computing devices, a plaintext representation of a particular parameter of a first of the computing devices, and a hashed representation of the same parameter of a second of the computing devices; hashing the plaintext representation of the particular parameter to create a hash value, and comparing the hash value to the hashed representation; and based on a determination that the hash value matches the hashed representation, correlating the hashed representation to the plaintext representation on the computer server system, wherein the code for reporting parameters of the computing devices includes code for allowing the computing devices to determine whether to send a plaintext representation or a hashed representation.

[0014] These and other implementations can optionally include one or more of the following features. The code for allowing the computing devices to determine whether to send a plaintext representation or a hashed representation can include biasing data that affects a frequency with which the computing devices select to send the plaintext representation or the hashed representation.

[0015] The method can further include receiving from the computing devices, plaintext representations and hashed representations of a plurality of different parameters of the computing devices; hashing the received plaintext representations to create hashed values; and using correlations between the hashed values and the received plaintext representations to identify parameters represented by the hashed representations. The method can further include using the hashed representation and the plaintext representation to identify characteristics of malware executing on the computing devices.

[0016] In some implementations, a computer-implemented method can include serving, from a computer server system and to a plurality of different computing devices remote from the computer server system, web code and code for reporting status of the computing devices; receiving from one or more of the computing devices, first data that indicates a parameter of the one or more computing devices,

the first data in a compressed format; receiving from one or more others of the computing devices, second data that indicates the parameter of the one or more others of the computing devices, the second data in an uncompressed format; and compressing the second data and comparing the compressed second data to the first data to correlate the first data to the second data, wherein the code for reporting status of the computing devices includes code for allowing the computing devices to determine whether to send the first data or the second data.

[0017] These and other implementations can optionally include one or more of the following features. The code for allowing the computing devices to determine whether to send the first data or the second data can include biasing data that affects a frequency with which the computing devices select to send the first data or the second data. The first data can be compressed on the computing devices using hashing. The server system can be configured to not send hashing algorithm information to the computing devices. The method can further include using the compressed format to represent the parameter in identifying aggregate activity by multiple of the computing devices. The method can further include determining from the aggregate activity by multiple of the computing devices whether ones of the multiple computing devices is infected with malware. The computer server system can be an intermediary security server system that is separate from a web server system that generates and serves the web code. The method can further include comparing information sent with the compressed second data to information derived from the received first data to determine whether the compressed second data was generated from data that matches the first data.

[0018] In some implementations, one or more non-transitory storage devices can store instructions that, when executed by one or more computer processors, perform operations comprising: serving, from a computer server system and to a plurality of different computing devices remote from the computer server system, web code and code for reporting status of the computing devices; receiving from one or more of the computing devices, first data that indicates a parameter of the one or more computing devices, the first data in a compressed format; receiving from one or more others of the computing devices, second data that indicates the parameter of the one or more others of the computing devices, the second data in an uncompressed format; and compressing the second data and comparing the compressed second data to the first data to correlate the first data to the second data, wherein the code for reporting status of the computing devices includes code for allowing the computing devices to determine whether to send the first data or the second data.

[0019] These and other implementations can optionally include one or more of the following features. The code for allowing the computing devices to determine whether to send the first data or the second data can include biasing data that affects a frequency with which the computing devices select to send the first data or the second data. The first data can be compressed on the computing devices using hashing. The operations can further include using the compressed format to represent the parameter in identifying aggregate activity by multiple of the computing devices. The operations can further include determining from the aggregate activity by multiple of the computing devices whether ones of the multiple computing devices is infected with malware.

The computer server system can include an intermediary security server system that is separate from a web server system that generates and serves the web code. The operations can further include comparing information sent with the compressed second data to information derived from the received first data to determine whether the compressed second data was generated from data that matches the first data.

[0020] In some implementations, a computer-implemented system includes: a first data communication interface arranged to communicate with a web server system; a second data communication interface arranged to communicate with clients that request content from the web server system; a compressed code interpreter programmed to identify an original form of compressed content received from particular ones of the clients by (a) compressing original content received from other ones of the clients to form a compressed representation, and (b) comparing the compressed representation to the compressed content received from the particular ones of the clients, wherein compressed code interpreter compresses the original content using a technique that matches techniques used by the particular ones of the clients to compress the content.

[0021] These and other implementations can optionally include one or more of the following features. The system can be further programmed to provide code to the clients that allows the clients to determine whether to provide compressed content or instead, uncompressed content to the system.

[0022] In some implementations, a computer-implemented method can include serving, from a computer server system and to a plurality of different computing devices remote from the computer server system, web code and code for reporting parameters of the computing devices; receiving from different ones of the computing devices, a plaintext representation of a particular parameter of a first of the computing devices, and a hashed representation of the same parameter of a second of the computing devices; hashing the plaintext representation of the particular parameter to create a hash value, and comparing the hash value to the hashed representation; and based on a determination that the hash value matches the hashed representation, correlating the hashed representation to the plaintext representation on the computer server system, wherein the code for reporting parameters of the computing devices includes code for allowing the computing devices to determine whether to send a plaintext representation or a hashed representation.

[0023] The features discussed here may, in certain implementations, provide one or more advantages. For example, a security intermediary system may be provided that does not add an appreciable level of bandwidth to the communication channel between a server system and the clients it services. The intermediary system may collect data that is relatively large compared to the bandwidth that it occupies, and may use that data for diagnosing problems with particular clients, and across large numbers of clients (e.g., by identifying the spread of malware threats). Moreover, a wide variety of data for various purposes may be transmitted using these techniques, and may be used for a wide variety of purposes once it is interpreted at the server system. Moreover, in certain implementations, the compressed representations can be used as database keys, thus further simplifying the operations recited herein.

[0024] Other features and advantages will be apparent from the description and drawings, and from the claims.

[0025] The appended claims may serve as a summary of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0026] In the drawings:

[0027] FIG. 1 is a schematic diagram of a system for providing compressed reporting of computing device information using a blind hash.

[0028] FIG. 2 is a schematic diagram of a system for performing deflection and detection of malicious activity with respect to a web server system.

[0029] FIG. 3 is a flow chart of a process for reducing bandwidth requirements between computers.

[0030] FIG. 4 is a swim lane diagram of a process for transferring data between client computers and a server system.

[0031] FIG. 5A is a representation of a state machine for client-side encoding.

[0032] FIG. 5B is a representation of a state machine for server-side decoding.

[0033] FIG. 6 is a block diagram of a generic computer system for implementing the processes and systems described herein.

[0034] Like reference numbers and designations in the various drawings indicate like elements.

DETAILED DESCRIPTION

[0035] In the following description, for the purpose of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, that the present invention may be practiced without these specific details. In other instances, well-known structures and devices are shown in block diagram form in order to avoid unnecessarily obscuring the present invention.

[0036] It will be further understood that: the term “or” may be inclusive or exclusive unless expressly stated otherwise; the term “set” may comprise zero, one, or two or more elements; the terms “first”, “second”, “certain”, and “particular” are used as naming conventions to distinguish elements from each other does not imply an ordering, timing, or any other characteristic of the referenced items unless otherwise specified; 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; that the terms “comprises” and/or “comprising” specify the presence of stated features, but do not preclude the presence or addition of one or more other features.

General Overview

[0037] This document discusses mechanisms for reducing bandwidth between client computing devices and server systems with which they communicate (where “clients” and “servers” are terms used generally, and do not require any sort of formal client-server architecture). Generally, the mechanisms are most useful where many different computing devices will be communicating the same data to the server system. For example, it may be beneficial to have computing devices report their configuration information to a server system so that the system can identify commonality in the operations of such devices, for example, to diagnose

reasons for faults in the devices or to identify the emergence of malware on the devices in a large group of devices (e.g., all devices that access a banking or retail web site).

[0038] The common data that is communicated may be communicated by some of the computing devices in its native form (e.g., plaintext) or another form in which its content can be directly determined (e.g., via lossless compression or encryption for which the server system receiving the data can accurately decompress or decrypt the data).

[0039] Others of the devices may communicate the same data in a form from which it cannot be identified directly, such as by submitted a hash of the data. When the server system receives compressed representations of the text but has not yet received the original representation, it can save indications of the compressed representations in association with the computing devices from which they were received, without knowing the original representation. When the server system receives any uncompressed representations, it can compress them using the same algorithm that the client devices used, can store the correlation of the compressed representation to the original representation, and can use that correlation to resolve any compressed representations, whether associated with events reported from computing devices in the past or the future, to determine what the compressed representation actually represents.

[0040] Some or all compressed representations may be accompanied by a secondary representation, that can be used to identify potential collisions between the compressed representation. In particular, because the compressed representations are smaller in size than the uncompressed representations, certain compressed representations will end up being repeated in a system—so that two identical compressed representations received by a server system could represent different original strings.

[0041] Though proper selection of parameters will make such collisions relatively rare, where the volume of the different strings that need to be represented is extensive, the risk of a collision may be relevant. The secondary representation, then, may serve as a check on the main representation, as it will be extremely unlikely that both would match even though the original text did not. Such secondary representation may be transmitted to the server system with the compressed representation, and may be formed, for example, by applying a second hash or other compression technique to the original text that uses a different algorithm, or by sending a value that represents a length of the original string.

[0042] The compressed representations or other representations that correspond to the compressed representations may then be passed as identifiers for the original data to systems that can perform analysis using such data. For example, client devices may pass reports that indicate anomalous activity, such as efforts by a browser plug-in to access served code using defunct function names or the like (e.g., in a system that uses a security intermediary to change the function names with each serving of the web code).

[0043] A fraud detection system may perform clustering analysis on the reported features of such computing devices, and may use the compressed representations as identifiers for the various reported features in performing such analysis. The analysis may be used to identify that device having particular characteristics (e.g., IP address, operating system, and browser) that have reported the existence of anomalous behavior, which may in turn be used to determine whether

the anomalous behavior is benign (e.g., from a plug in that users intentionally installed) or malicious (e.g., code performing a “Man in the Middle” attack on their devices).

[0044] FIG. 1 is a schematic diagram of a system 100 for providing compressed reporting of computing device information using a blind hash. In general, the system 100 is directed to presenting information from a web server system 108 to a variety of computing devices 114A-C that are located remotely from the web server system 108.

[0045] Examples of operators of such a web server system 108 include on-line retailers and on-line banking systems, where the devices 114A-C belong to people trying to buy products or perform on-line banking transactions. The web server system 108 is shown as a row of servers along with a separate row of servers for a security server system 106, both in a single data center facility. Such arrangement is intended to indicate that, in one typical implementation, an operator of a web site may supplement its main server system 108 with a security server system 106 that it builds itself or that it acquires for a third party.

[0046] The security server system 106 may physically and logically between the web server system 108 and the network, which may include internet 104, and may intercept web code to be served to the various client devices 102A-C.

[0047] In the described example, the system 100 operates by providing modified or recoded web code to the client computing device 102, where the modifications are relative to a web page that would normally be served to the client computing device without additional security measures applied. Web code may include, for example, HTML, CSS, JavaScript, and other program code associated with the content or transmission of web resources such as a web page that may be presented at a client computing device 102 (e.g., via a web browser or a native application (non-browser)).

[0048] The system 100 can detect and obstruct attempts by fraudsters and computer hackers to learn the structure of a website (e.g., the operational design of the pages for a site) and exploit security vulnerabilities in the client device 102. For example, malware may infect the client device 102 and gather sensitive information about a user of the device, or deceive a user into engaging in compromising activity such as divulging confidential information. Man-in-the-middle exploits are performed by one type of malware that is difficult to detect on a client device 102, but can use security vulnerabilities at the client device 102 to engage in such malicious activity.

[0049] Served code 110 shows an example of code that can be served to a requesting one of various of the computing devices 102A-C after the request is provided to the web server system 108, the content from the web server system 108 is intercepted or otherwise provided to the security server system 106, and the code is changed and/or supplemented by the security server system 106. Various portions of the served code 110 are shown schematically to actions that the security server system 106 can take with respect to the code.

[0050] Code 110A represents the original web code provided by the web server system 108 with certain modifications made to it. For example, the security server system 106 may change the names of functions in essentially random ways every time a set of content for a web page is served, where the changes are made consistently across the served code so as not to break internal references between pieces of the code. For example, references to a particular function

may be made consistently across HTML, CSS, and JavaScript. For example, the following strings indicate HTML before and after alteration using a random number for textual replacement:

[0051] Original code:

```
<form action="login.jsp" method="post" name="Login">
<input type="text" id="lastname_id" name="lastname" Re-coded format:
<form action="login.jsp" method="post" name="imp0q6wNm">
<input type="text" id="b24mpqdfkX" name="aSkFjp5x1Y"
```

[0052] Such changes may be made so that malware on a client device that receives the code cannot easily identify the operational structure of the web site and/or automatically interact with the code so as to mislead a user into opening its security to the malware (e.g., for a Man in the Middle attack). By making the changes frequently enough and randomly enough that automated malware cannot interact with it predictably, the security server system **106** interferes with such attacks by malware.

[0053] Instrumentation code **110B** is added to the code **110A** by the security server system **106**, and allows the system **100** to detect malware in addition to deflecting its efforts. In particular, the instrumentation code **110B** can execute in the background on the computing devices **102A-C** and can monitor how the code **110A** operates and how other code on the particular computing device **102A-C** interacts with the execution of code **110A**. For example, the instrumentation code **110B** can monitor the DOM made from the code **110A** at different points in time and may report back to security server system **106** information that characterizes the current state of the DOM. Such information can be compared to information that indicates what the DOM should look like in order to determine whether other side is interfering with the execution of code **110A**. Alternatively, or in addition, the instrumentation code can identify anomalous attempts by third-party code to interact with the operation of code **110A**, such as for calls made to code **110A** using "old" names for the code (e.g., names that were valid in a prior serving of the relevant web page but that are no longer relevant because security server system **106** is constantly changing the names so as to create a moving target for such third-party code to hit).

[0054] A user telemetry script **110C** is also provided to a requesting one of computing devices **102A-C**. The user telemetry script **110C** may include code for managing communications between the relevant client device and the security server system **106**. Such communications may include transmission of information identified by the instrumentation code **100B** described above, and other relevant information. In certain implementations, the security server system **106** can be supplied additional information using the user telemetry script and after the code **110A** has been served, such as information that affects the manner in which the instrumentation code **110B** operates. For example, the security server system **106** may receive a report from the user telemetry script **110C** that indicates that a third-party program is attempting to interact with the served code **110A**, and may respond so as to have the instrumentation code **110B** perform certain operations to better understand the nature of the interaction occurring on the computing device.

[0055] A request frequency code **110D** may also be sent and may be as simple as a single number that biases the user telemetry script **110C** to return information to the security

server system **106** in its original form, or instead in a compressed form. For example, the request frequency code **110D** that is sent in this example is a value of 1000, which may have been selected by the security server system **106** for a range between 0 and 1024 in this example. In turn, the user telemetry script **110C** may be programmed to select a random number between 0 and 1024, and to return the original text rather than a compressed version of the original text when the randomly-selected number exceeds 1000. As a result, original text will be returned by only about 2% of all computing devices that are served code from the security server system **106** using this request frequency value. Others of the computing devices will return a compressed version of the text, such as a hash of the original text produced by the particular device.

[0056] Upon receiving the code **110**, the particular client devices **102A-C** may render respective webpages and establish document object models that represent the served page, in a familiar manner. User interactions with the webpage and associated code may then begin. At or around that time, the instrumentation code **110B** and user telemetry script **110C** may execute to return information about the configuration of a particular computing device to the security server system **106**. For example, the user telemetry skip script **110C** may return data that identifies the operating system of the particular computing device, the model of the particular computing device, the amount of RAM loaded on the computing device, other applications executing on the computing device, and similar information. In certain implementations, such functionality may be provided using a browser plug in that is programmed to perform a check of the environment for the machine on which it is running. Generally, JavaScript or VBScript can permit that measurement of User Agent, other HTTP header information, indirect measurements of the JavaScript execution environment, Plugin information, fonts, and screen information.

[0057] As shown by the arrow labeled with a 1 in a circle, computing device **102A** returns the numeric pair 24.16. These numbers represent, respectively, a hash of a textual string that represents the name and model of the browser that is running on computing device **102A**. In the example here, all three computing devices **102A-C** are running the "Chrome 2.3.21.04" browser release, as an example. Such information may be obtained by making a request that is to be responded to with the "user agent" string on the particular computing device, in a familiar manner. In the current example, computing device **102A** delivered this compressed representation of the user agent string, because it generated a random number of 300, which is less than the request frequency number of 1000.

[0058] Similarly, when computing device **102B** received the served code **110**, it generated a random number of 674, meaning that it too would send a compressed version of the user agent string, or 24.16. In both these examples, 24 has been selected as an example to represent a hash that may be created from such a string, and the number 16 represents the number of characters in that string.

[0059] The actual string itself can be seen as being transmitted from computing device **102C** back to security server system **106**. Here, computing device **102C** selected a random number of one 1012, which is greater than the request frequency number of 1000. As a result, computing device

102C will be one of the 2% of all devices that report back the original, uncompressed (unhashed) version of the user agent string.

[0060] To better show the level to which an initial string can be compressed, the user agent string for Firefox on an Ipad is “Mozilla/5.0 (iPad; U; CPU OS 3_2_1 like Mac OS X; en-us) AppleWebKit/531.21.10 (KHTML, like Gecko) Mobile/7B405.” A compressed representation that indicates a hash and a length might be of the form 4528.111. As can be appreciated, the bandwidth for the latter is much lower than for the former.

[0061] In the figure, operations of the security server system **106** performed in response to receiving the communications from devices **102A-C** are shown schematically as a two-column database entry below security server system **106** and Web server system **108**. The two columns are shown to indicate how a system may associate a compressed version of a string with the actual string itself. In a first representation shown by a 1 in a circle and corresponding to actions that would occur in response to the first transmission from computing device **102A**, the database has been populated with the hash value of 24 upon receiving that hash value form device **102A**. The system **100** does not, at that point, know what the original string representation for that value is (assume that the system did not receive earlier communications regarding the user agent string from other device), but stores the hash value 24 in anticipation that will eventually be able to determine what the original, plaintext value is.

[0062] In a second representation shown by the number 2 in a circle and representing the transmission from computing device **102B**, the table has not changed because again, the security server system **106** received only the hash code, and not the original version of the user agent string. Finally, at the bottom of the representation, the system receives a string of original plaintext and, as shown by the arrow labeled with “hash,” the system performs a hashing function on that plaintext that is the same as a hashing function that the system **100** knew to be provided by the computing devices **102A-C**. For example, each of the computing devices **102A-C** and the security server system **106** may be programmed to use the same hashing algorithm as the Java hash algorithm, which is well known and readily available on many computing platforms.

[0063] With that hash value (24) in hand, the security server system **106** may search the table for a matching value, and when it finds such a matching value, it may determine that that matching hash value is what corresponds to the original text. It may then update the table to correlate the particular hash value with the particular original plaintext. Such a correlation is shown in the row of the table labeled with a 3 in a circle.

[0064] This correlation may then be used with other parts of the system. For example, the number 24 can be used throughout the system to represent the user agent string represented here (i.e., as a unique database index value). As some examples, a cluster analysis system like that discussed with respect to FIG. 2 below may use the number 24 to represent such a feature instead of using the full string representation. In other embodiments, yet a third representation for the feature may be used as an index representation.

[0065] The processing of the communication from computing device **102C** may also be accompanied by a determination that the full string is 16 characters in length. Such

a value may be stored in yet a third column of the table (not shown) and may be correlated to the hash value and the original plaintext of the string. When later communications arrive with a hash value of 24, they may be compared to the first column shown in the table, and their accompanying value of 16 may be compared to this additional value to provide more confidence that the hash value is unique to this particular original textual string. As discussed above, other techniques may also be used to ensure that there are no collisions in the hash values, such as by returning an additional number or other representation that is generated by an alternative hash algorithm. In certain implementations, if the security server system **106** identified that there may be a problem with a received hash value, the security server system **106** may provide a special message to the responding computing device to trigger the responding computer device to transmit the original plaintext code instead of the hash value.

[0066] Other tables may store additional relationships that are of value in operating the system **100**. For example, one table may store identifiers for particular ones of the computing devices **102A-C**, where a particular device may be identified by a cookie that it stores and passes to the security server system **106**. That device identifier may then be related to the variety of parameters, such as the user agent parameter just discussed, and additional parameters, which may include hardware identifiers, operating system identifiers, and software identifiers, among other things. By this mechanism then, the system **100** may correlate a particular device to particular configuration information and to configuration parameters reported by the device.

[0067] This particular example is highly simplified for purposes of clarity. In a typical implementation, many different webpages and other Web resources will be served by system **100** to many different computing devices. Thus, a large number of different hash values will be received by security server system **106** in an interleaved fashion with each other, and the system will need to correlate those hash values or other compressed values with particular original text represented by those values. Such multi-value implementation may occur, for example, by adding additional records to the simple table shown here, or by other appropriate techniques.

[0068] A server system can also specify a seed to be used before generating a random number, or specify another random number generation method (and the initial state of the pseudorandom number generator (PRNG), and the choice threshold value, such that the sequence of fields chosen will be known by the server. This can be used to force the client to generate an “uncompressed” value for a field that is unknown by the client. It can also be used to allow the server to have more control over the data flow (more or less data), and can even be used as a mechanism for determining when a malicious client is sending data in a non-compliant format, which could be used to determine that the client is, in fact, addled with malware.

[0069] From time to time, hash values that have already been correlated with original text may also be tested by other incoming original text. For example, the security server system **106** might not normally perform a hash on incoming original text if the system **106** has determined that there is already a correlation for that text in the table.

[0070] However, a random number approach similar to that used on the computing devices **102A-C** may be used so

that the security server system **106** periodically does perform such a hashing and comparison so as to confirm the accuracy of the data in the table. If the system **106** determines that there is an inaccuracy, because the hash value generated for an incoming string of text does not match a pre-existing hash value in the system for that text, the system **106** may generate an exception and alert an operator of the system **106**.

[0071] Also, the example here is stated in terms of Web code being served to a general web browser. Other types of code may alternatively be served to other types of applications. In such situations, those other applications may be caused to choose whether to return original or compressed configuration information, or such decisions may be made by code separate from the applications but made in respect to the execution of the applications.

[0072] Also, although the techniques discussed here have been associated with communications for the delivery of information related to browser environment and user or automated interactions with web pages, they may also, in appropriate circumstances, be applied more generally. For example, other data that is reported at periodic intervals and is common as between a substantial portion of those reporting events, may be compressed using the techniques here, and interpreted using uncompressed (or losslessly compressed) messages in some instances of the reporting, and lossy compressed messages corresponding to the same content in other instance of reporting. Various mechanisms, including those discussed above and below, may be used to identify that the compressed and uncompressed messages match each other in their content, and to then associate the compressed messages with the uncompressed content.

[0073] In addition, while the techniques are described here as involving transmission of data to a server system from web code served to a browser, other techniques may also be used. For example, a stand-alone application for a particular organization may report information to a server system, and may be programmed to use the sometimes-compressed/sometimes-uncompressed techniques described here to transmit necessary data to the server system (particularly when the data is largely repetitive as between different reporting events for the data).

[0074] FIG. 2 is a schematic diagram of a system **200** for performing deflection and detection of malicious activity with respect to a web server system. The system **200** may be the same as the system **100** discussed with respect to FIG. 1, and is shown in this example to better explain the interrelationship of various general features of the overall system **200**, including the use of the reporting of compressed and uncompressed versions of the same strings in order to conserve bandwidth (for compressed representations) and to determine what the compressed representations represent (for uncompressed representations).

[0075] The system **200** in this example is a system that is operated by or for a large number of different businesses that serve web pages and other content over the internet, such as banks and retailers that have on-line presences (e.g., on-line stores, or on-line account management tools). The main server systems operated by those organizations or their agents are designated as web servers **204a-204n**, and could include a broad array of web servers, content servers, database servers, financial servers, load balancers, and other necessary components (either as physical or virtual servers).

[0076] A set of security server systems **202a** to **202n** are shown connected between the web servers **204a** to **204n** and a network **210** such as the internet. Although both extend to n in number, the actual number of sub-systems could vary. For example, certain of the customers could install two separate security server systems to serve all of their web server systems (which could be one or more), such as for redundancy purposes. The particular security server systems **202a-202n** may be matched to particular ones of the web server systems **204a-204n**, or they may be at separate sites, and all of the web servers for various different customers may be provided with services by a single common set of security servers **202a-202n** (e.g., when all of the server systems are at a single co-location facility so that bandwidth issues are minimized).

[0077] Each of the security server systems **202a-202n** may be arranged and programmed to carry out operations like those discussed above and below and other operations. For example, a policy engine **220** in each such security server system may evaluate HTTP requests from client computers (e.g., desktop, laptop, tablet, and smartphone computers) based on header and network information, and can set and store session information related to a relevant policy. The policy engine **220** may be programmed to classify requests and correlate them to particular actions to be taken to code returned by the web server systems (for transmission to requesting clients) before such code is served back to a client computer. When such code returns, the policy information may be provided to a decode, analysis, and re-encode module **224**, which matches the content to be delivered, across multiple content types (e.g., HTML, JavaScript, and CSS), to actions to be taken on the content (e.g., using XPATH within a DOM), such as substitutions, addition of content, and other actions that may be provided as extensions to the system. For example, the different types of content may be analyzed to determine naming that may extend across such different pieces of content (e.g., the name of a function or parameter), and such names may be changed in a way that differs each time the content is served, e.g., by replacing a named item with randomly-generated characters. Elements within the different types of content may also first be grouped as having a common effect on the operation of the code (e.g., if one element makes a call to another), and then may be re-encoded together in a common manner so that their interoperation with each other will be consistent even after the re-encoding.

[0078] A rules engine **222** may store analytical rules for performing such analysis and for re-encoding of the content. The rules engine **222** may be populated with rules developed through operator observation of particular content types, such as by operators of a system studying typical web pages that call JavaScript content and recognizing that a particular method is frequently used in a particular manner. Such observation may result in the rules engine **222** being programmed to identify the method and calls to the method so that they can all be grouped and re-encoded in a consistent and coordinated manner.

[0079] The decode, analysis, and re-encode module **224** encodes content being passed to client computers from a web server according to relevant policies and rules. The module **224** also reverse encodes requests from the client computers to the relevant web server or servers. For example, a web page may be served with a particular parameter, and may refer to JavaScript that references that

same parameter. The decode, analysis, and re-encode module 224 may replace the name of that parameter, in each of the different types of content, with a randomly generated name, and each time the web page is served (or at least in varying sessions), the generated name may be different. When the name of the parameter is passed back to the web server, it may be re-encoded back to its original name so that this portion of the security process may occur seamlessly for the web server.

[0080] A key for the function that encodes and decodes such strings can be maintained by the security server system 202 along with an identifier for the particular client computer so that the system 202 may know which key or function to apply, and may otherwise maintain a state for the client computer and its session. A stateless approach may also be employed, whereby the system 202 encrypts the state and stores it in a cookie that is saved at the relevant client computer. The client computer may then pass that cookie data back when it passes the information that needs to be decoded back to its original status. With the cookie data, the system 202 may use a private key to decrypt the state information and use that state information in real-time to decode the information from the client computer. Such a stateless implementation may create benefits such as less management overhead for the server system 202 (e.g., for tracking state, for storing state, and for performing clean-up of stored state information as sessions time out or otherwise end) and as a result, higher overall throughput.

[0081] An instrumentation module 226 is programmed to add instrumentation code to the content that is served from a web server. The instrumentation code is code that is programmed to monitor the operation of other code that is served. For example, the instrumentation code may be programmed to identify when certain methods are called, when those methods have been identified as likely to be called by malicious software. When such actions are observed to occur by the instrumentation code, the instrumentation code may be programmed to send a communication to the security server reporting on the type of action that occurred and other meta data that is helpful in characterizing the activity. Such information can be used to help determine whether the action was malicious or benign.

[0082] The instrumentation code may also analyze the DOM on a client computer in predetermined manners that are likely to identify the presence of and operation of malicious software, and to report to the security servers 202 or a related system. For example, the instrumentation code may be programmed to characterize a portion of the DOM when a user takes a particular action, such as clicking on a particular on-page button, so as to identify a change in the DOM before and after the click (where the click is expected to cause a particular change to the DOM if there is benign code operating with respect to the click, as opposed to malicious code operating with respect to the click).

[0083] Data that characterizes the DOM may also be hashed, either at the client computer or the server system 202, to produce a representation of the DOM (e.g., in the differences between part of the DOM before and after a defined action occurs) that is easy to compare against corresponding representations of DOMs from other client computers.

[0084] Other techniques may also be used by the instrumentation code to generate a compact representation of the

DOM or other structure expected to be affected by malicious code in an identifiable manner.

[0085] The instrumentation module 226 or another component may also provide a user telemetry script or other code for causing the client device receiving the other code to communicate with the server system after the code is transmitted. Such additional code may include code that causes the client devices to return configuration information about themselves, and to control whether they return the information in a compressed or native state, in the manners described above. The module 226 may also generate and provide to the client devices a request frequency value that helps control how often the native text is transmitted back to the system instead of the compressed form of the text. One or more modules may also control the receipt of such configuration information, the storage of the information, and the correlation of the compressed data (e.g., being used as an index value for a table) and the corresponding original form of the data.

[0086] As noted, the content from web servers 204a-204n, as encoded by decode, analysis, and re-encode module 224, may be rendered on web browsers of various client computers. Uninfected client computers 212a-212n represent computers that do not have malicious code programmed to interfere with a particular site a user visits or to otherwise perform malicious activity. Infected client computers 214a-214n represent computers that do have malware, or malicious code (218a-218n, respectively), programmed to interfere with a particular site a user visits or to otherwise perform malicious activity. In certain implementations, the client computers 212, 214 may also store the encrypted cookies discussed above and pass such cookies back through the network 210. The client computers 212, 214 will, once they obtain the served content, implement DOMs for managing the displayed web pages, and instrumentation code may monitor the respective DOMs as discussed above. Reports of illogical activity (e.g., software on the client device calling a method that does not exist in the downloaded and rendered content) can then be reported back to the server system.

[0087] The reports from the instrumentation code may be analyzed and processed in various manners in order to determine how to respond to particular abnormal events, and to track down malicious code via analysis of multiple different similar interactions across different client computers 212, 214. For small-scale analysis, each web site operator may be provided with a single security console 207 that provides analytical tools for a single site or group of sites. For example, the console 207 may include software for showing groups of abnormal activities, or reports that indicate the type of code served by the web site that generates the most abnormal activity. For example, a security officer for a bank may determine that defensive actions are needed if most of the reported abnormal activity for its web site relates to content elements corresponding to money transfer operations—an indication that stale malicious code may be trying to access such elements surreptitiously.

[0088] A central security console 208 may connect to a large number of web content providers, and may be run, for example, by an organization that provides the software for operating the security server systems 202a-202n. Such console 208 may access complex analytical and data analysis tools, such as tools that identify clustering of abnormal activities across thousands of client computers and sessions,

so that an operator of the console **208** can focus on those clusters in order to diagnose them as malicious or benign, and then take steps to thwart any malicious activity.

[0089] In certain other implementations, the console **208** may have access to software for analyzing telemetry data received from a very large number of client computers that execute instrumentation code provided by the system **200**. Such data may result from forms being re-written across a large number of web pages and web sites to include content that collects system information such as browser version, installed plug-ins, screen resolution, window size and position, operating system, network information, and the like. In addition, user interaction with served content may be characterized by such code, such as the speed with which a user interacts with a page, the path of a pointer over the page, and the like. The telemetry data may also include the received data that characterizes the then-current conditions of each of the client devices, such as the browser and operating systems that they were running, and other appropriate information.

[0090] Such collected telemetry data, across many thousands of sessions and client devices, may be used by the console **208** to identify what is “natural” interaction with a particular page that is likely the result of legitimate human actions, and what is “unnatural” interaction that is likely the result of a bot interacting with the content.

[0091] Statistical and machine learning methods may be used to identify patterns in such telemetry data, and to resolve bot candidates to particular client computers. Such client computers may then be handled in special manners by the system **200**, may be blocked from interaction, or may have their operators notified that their computer is potentially running malicious software (e.g., by sending an e-mail to an account holder of a computer so that the malicious software cannot intercept it easily).

[0092] FIG. 3 is a flow chart of a process for reducing bandwidth requirements between computers. In general, the process involves providing client computers with code that causes the computers to report back aspects of their operation. Different ones of the client computers are caused to report the information in compressed form, while others of the client devices are caused to report the same information in an original uncompressed, or plaintext form. The process can then use the combination of compressed and uncompressed reported information to correlate the compressed representations with the uncompressed representations, even though no particular computer or transmission provided such a correlation for the server system that served the code. The server system may make the correlation, for example, by performing a compression of received uncompressed code in a manner that matches the way that one or more of the client devices performed the compression of the same code or data.

[0093] The process begins at box **302**, where the server system serves Web code to a plurality of different client devices. The Web code may be code for a particular webpage, for multiple related webpages, or for various unrelated webpages associated with different websites, including websites from different domains. In certain implementations, the Web code may be recoded from what is initially served by a Web servers, such as by rewriting the names of particular functions or other elements in unpredictable manners but in a way that is consistent across all of the elements being served (e.g., so that the code does not break when executed

and so that calls made to a particular function or other element are changed according to the changes made in the name of the element).

[0094] At box **304**, supplemental code is served by the system. The supplemental code may be served along with the Web code in a single transaction, or may be served separately. The supplemental code may include, for example, instrumentation code and telemetry code that causes the receiving client device to monitor the operation of the Web code that is served to the device and potentially to report back on such operation to a security server system, if the monitoring determines that anomalous activity is occurring on the client device. Other code may also be served, such as parameter values that may affect the way in which the supplemental code operates, such as a request frequency number described above, and other appropriate values.

[0095] At box **306**, the server system may have waited after serving both the Web code and the supplemental code, and may subsequently receive, from the client or clients to whom the code was served, hashed representations for configuration. Those representations may represent a variety of parameters that are relevant to the client devices from which they come, including identifiers for the current configuration state of a particular client device. The particular parameter may be identified, and the value of the identified may be identified by the hash code that one of the client devices generated by hashing the plaintext parameter value. A number of different parameters may be reported on for each client device, and even more parameters may be reported on across a universe of client devices. For example, Web code served from a certain webpage may be accompanied by instrumentation code that reports back on certain parameters of a device, while Web code served for another webpage may be accompanied by code that reports back on other parameters.

[0096] When the system receives such hashed representations, it may save them, as shown at box **308**, even though it does not at that time know what original values they represent. Such representations may also be associated with identifiers for client devices from which they were received, so that the particular configuration information for those devices may be determined later, even if it cannot be determined when the hashed representations are initially received.

[0097] At box **310**, plaintext representations are received from one or more client devices. The plaintext representations may have been transmitted by those client devices in response to the client devices executing instrumentation or telemetry code that instructed the transmission of such plaintext versions of the information to be transmitted (e.g., upon the client device choosing to transmit plaintext rather than a compressed representation). When the security system receives plaintext representations from telemetry code, it may be programmed to first compress those plaintext representations such as by hashing them. The compression may occur according to a mechanism that matches a known hashing mechanism to be operating on the client devices in cooperation with the instrumentation and telemetry code that was served to those client devices.

[0098] With the plaintext representations having been hashed, the security system will now have a correlation between a particular plaintext representation and a particular hash value. The system may then compare that hash value to any of the hashed values that have previously been received,

at box 314, and may then correlate whatever previously-received hash values were received to the plaintext representation that was later received, at box 316. In certain examples, the initial transfer of a particular piece of data may be in plaintext form, so that the database would be populated with a plaintext representation and a hash representation simultaneously. Later transmissions of plaintext representations may simply be matched against the plaintext column of the database, and the devices that sent those plaintext representations may be correlated with the hashed value as an index value for those devices. Alternatively, the plaintext values that are later received may always be hashed, and the hashed values may be compared against the database if that is a more efficient operation of the system computationally. Also, periodically, plaintext representations and their hash values may be checked against the table to ensure that there are no errors in the data. In addition, other values that represent the plaintext may be transmitted along with the hashed representations of the plaintext so as to ensure that the system is not receiving overlapping hash values that match each other but that each represent different plaintext representations.

[0099] At box 318, characteristics of infected computers are identified using information gleaned from the previous steps. For example, the hashed values may be used as data in statistical analysis techniques, such as techniques that may attempt to identify clusters of activity within a population of computers, such as a population of hundreds of thousands of computers. Clustering may indicate anomalous activities by those computers, and the hash values may then be used to determine what configuration information is possessed in common by computers within that cluster. As one example, the analysis may determine that a large majority of computers having anomalous behavior are running a recently released operating system or browser version (i.e., that anomalous behavior is clustered around a dimension associated with that particular value of the user agent parameter for a population of machines). Such a determination may be evidence of a vulnerability of such browser or operating system version to Mal Ware. An operator of the system described here may then act upon such information, such as to cause the browser or operating system to be updated or the security hole to otherwise be plugged.

[0100] FIG. 4 is a swim lane diagram of a process for transferring data between client computers and a server system. In general, the process, like those discussed above, involves transmitting content to a server system, in most instances, in a compressed manner from which the identity of the original content cannot be determined (a lossy compression like forming a hash). In a small number of cases, the content can be transmitted in an uncompressed or losslessly compressed form, the received data may be compressed using a process equivalent to the process that was used by clients on the other received content, and the compressed form may be matched to the compressed forms received in that other received content. In this way, the original form of the other received content (both past and future) can be inferred.

[0101] The process begins at box 402, where a client device requests a web page, such as via a GET or POST method. Such a request may be directed to a particular URL served by a web server system of a particular organization. The request may result in the web server system identifying appropriate code to respond to the request, which may

include static code and dynamic code, and may take the form of HTML, CSS, and JavaScript, among others. At box 404, the web server system serves the responsive code.

[0102] The served code is intercepted at box 406 by a security server system that, e.g., the operator of the web server system has added as an intermediary for providing security for the web server system. For example, a third party may provide a security system that can be added modularly to a company's web server system without having to affect the web server system in any substantial manner. In other implementations, the intermediary functionality may be integrated in the web server system. Also, the intermediary server system may be physically location within the same building as the web server system (for minimizing latency and maximizing the ability to coordinate systems) or in a separate location that requires communication through a network, including the Internet,

[0103] At box 406, the security server system intercepts the code and modifies it. For example, as described above, the names of certain functions may be changed in a sufficiently random or arbitrary manner that the new names cannot be anticipated by malware running on the clients. The changes may be coordinated across different types of code (e.g., HTML, CSS, and JavaScript) where the names occur, so that the code functions the same as the code it replaced. Generally, the changes are made to latent code whose operation a user does not see, and static code.

[0104] At box 408, the code is appended with monitoring and reporting code. Such code may monitor the DOM that is created on the client when the served code is rendered, or may monitor attempts to interact with the code, and may characterize and report any abnormal activity. Such code may also report other status information about a client, such as configuration information that describes the features of the client system. In certain situations, a complete picture of what is occurring in the browser or other application (e.g., a specific app programmed for the company that serves the code). The reporting code may in particular include code for making a determination whether to report particular information in a compressed versus an uncompressed form, and then to transmit the data back to the server system accordingly.

[0105] At box 410, the client renders the web page by executing the various types of served code, and perhaps by acquiring code from other sources in addition to the code that was initially served by the web server system (whether from the organization that operates the web server system or from one or more other organizations). As described throughout this process, the serving and executing of code described here would be repeated across thousands or more different client devices that may each vary in different ways, such as by having different base (the basic computer) and extended hardware (e.g., added graphics cards or RAM), operating systems, installed and executing applications, and executing browser plug ins. Thus, each rendering of the web page may be performed in a different manner for different ones of the client devices, and even for the same client device in different sessions.

[0106] At box 412, the client device generates characterization and activity data that is to be sent back to the server systems. The box is labeled with a "1" to indicate that this step represents a subset of the devices that are served the web code, and are the devices that hash the data that is to be reported so as to lower the bandwidth required for such

reporting. Generally, the vast majority of instances would be established to report in such a manner so as to significantly reduce the overhead of transmitting the data.

[0107] In this example, characterization data represents status of the client device, such as hardware and software on the device, whereas activity data represents actions that have occurred on the device, particularly since the device received the served web code (e.g., activities between the served code and other code that is on the device). The characterization data may be sent to one server system, while the activity data may be sent to another, or they may be sent to the same server system. Also, certain data may be sent according to the compressed/uncompressed scheme described in this document when the data is expected to be common across many devices, so that the original value of the content for devices that compress their content can be inferred from the uncompressed content (where, unless otherwise noted, uncompressed content includes content whose original form can be determined by a server system that receives it, and thus includes losslessly compressed content). Other data may be sent in a normal manner, without the pairing of compressed/uncompressed transmission, such as where the content is not typically common as among different machines, so that there would be relatively little value in trying to infer the original content from transmissions made by other machines.

[0108] At box 414, an analysis system receives the reported data, which may include activity data. The analysis system may use such activity data to identify that certain normal or anomalous activities have occurred on a certain device, and may conduct analysis on similar activity data received from a large number of other devices to identify clusters of common activity so as to determine that malware is taking advantage of such devices. The analysis system may also be provided with characterization data so that it can determine characteristics of the devices that are being affected by the malware.

[0109] Separately, or as part of the same communication, the client device may provide similar data to the security server system, as indicated at box 416. The security server system may then associate the particular client device with the hashed forms of the compressed content that is sent (as the analysis system may do if it receives only hashed data). At this point in the example process, the security server system has received no unhashed form of the content, so it does not know what the original form of the content was. As a result, the system may simply associate an identifier for the particular device with the hashed form of the received content (or may simply index upward a count of the number of clients reporting the content of the particular form of hash). In this example, multiple different fields may be reported in a hashed manner, such as one or more fields that identify hardware for a device, and one or more fields that identify software executing on the device. Each feature of the device (e.g., make and model, operating system, amount of RAM, etc.) may receive its own hash, or groups of features may receive a single hash—where each hash is selected so as to cover content that is likely to be common across many devices, so that the hash value may be readily reverse-engineered when an uncompressed version of the content is received from another device.

[0110] At box 418, another client (indicated by the circled “2”) also generates and reports characterization and activity data. In this instance, the particular device does not com-

press the content that it reports—e.g., because it selected a number pseudo-randomly that does not exceed a predetermined level that was provided with the web page code. The analysis system may receive at least some of the generated content at box 420 (which may be the same content as received at box 414 or may contain some fields whose parameters are the same as those received at box 414), though here the content would be received in uncompressed form (e.g., either as plaintext or in a losslessly compressed format). To the extent the analysis system previously received parameters for certain fields in compressed format, it may compress the received uncompressed content to form a hash value and may then compare it to compressed content that was previously received. If the hash value matches a hash value stored from Box 414, then the original content may be associated by the system with the other devices that previously reported the hashed value, as may future devices that report the hashed value. Alternatively, or in addition, the analysis system can add to a number of devices that have reported as having the particular parameter.

[0111] Similarly, the second client device can report the characterization and activity data to the security server system, and at box 422, that system can generate a hash value for it. As with the analysis system, certain other fields may have been reported in hashed form or may always be reported by all devices in uncompressed form.

[0112] At box 424, the security server system associates the particular parameters received from box 412 with the other instances of reporting the same content (as determined by comparing the just-generated hash value with previously-received hash values from the other devices).

[0113] In situations where the analysis system does not separately track associations between particular device IDs and content reported by those devices, the analysis system can request ID and parameter data (box 426) from the security server system. The security server system (box 428) may gather and transmit such data, and the analysis system may identify common features of anomalously-acting machines (box 430) using such data. In other words, in one implementation, the analysis system may receive activity data and use such data to identify clusters of common activity, or otherwise identify potential problems that arise in the operation of a number of different client devices. At the time of such initial analysis, the analysis system may not know the characterization data for the devices, and may only seek such data from the security server system after identifying the problem. Such follow-up information gathering may then be used by the analysis system to identify features of the devices that are determined to be acting anomalously, such as by determining that they all are executing the same browser program, and perhaps a common version or range of versions of that program. In yet other embodiments, the analysis system may repeat operations that are performed by the security server system, such as in the inferring of the original content of compressed messages via compressing of received uncompressed messages.

[0114] Also, the security server system and the analysis server system may be part of the same system or separate systems. For example, a retailer may manage both systems along with a web server system. In another example, a third-party may operate the analysis server system from its own facility, and can assist customers with operating their particular security server systems on their premises, with their web server systems. The third-party may aggregate

activity over a large number of served content in such manner, and may more readily identify anomalous behavior than could a single organization serving only a fraction of such content.

[0115] FIGS. 5A and 5B show, respectively, state diagrams for a client and a server operating according to the mechanisms described above. Referring specifically to the client encoding state machine of FIG. 5A, at box 502, the client device begins its operations by which it prepares information for transmission to the server system and performs the transmission. At box 504, a determination is made whether more fields need to be encoded for transmission. If not, then the client waits until a next time that processing and transmission is needed.

[0116] At box 506, if more fields need to be transmitted to the server, a random number (which may be pseudorandom or otherwise less than exactly random) is generated at box 506. The number may be generated for each overall transmission or for each field within a transmission (so that some field values may be compressed and some not). At box 508, the client determines whether the generated number exceeds a threshold. That threshold may be a predetermined value that is relatively permanent and stored by the client for a long time, or may be highly variable, where the threshold is transmitted with code recently received by the client, or is accessed at run time by the client (e.g., by submitting a GET function to a remote server system). If the generated number exceeds the threshold, then the client sends a raw version of the relevant field, such as in plaintext or losslessly compressed form of the content for the field (box 512). If the threshold is not exceeded, then a hashed version of the content is sent (box 510). Of course, the determination may be made inversely, so that the hashed form is sent if the threshold is exceeded (and/or matched), and the raw data is sent if it is not (and/or is matched).

[0117] Referring now to FIG. 5B, there is shown a state diagram for a server that interacts with the operations of the client just described. At box 520, the process begins, such as by the server determining that it has received data for a plurality of fields, where the data needs to be interpreted by the server system. If there are no more fields to process, the system returns to a rest state, but if there are, then the server analyzes the next field in line and determines whether it is in raw form or hash form (box 524). If it is in raw form, then the server hashes the field using a hashing technique that matches a technique that the server knows to be performed by various clients that are reporting data to it (box 532). The server then associates the hash result with the raw content (box 534). The system can then use such a correlation between the hash result and the raw data to interpret other communications from other clients that contain only the hash result. In particular, the system can use the correlation to infer what the raw form at the client was when only the hash form is received.

[0118] If the field is not in raw form (is in hash form), the system performs a lookup on the hash form (box 526). The system determines whether the hash form of the field is found in the system (box 528), so as to indicate that a correlation has already been stored between the hash form and the raw form. If the hash form is found, then the system can get the raw value a(box 530) and act accordingly. If the field is not found (e.g., because the value for the field has not previously been received in raw form), then the occurrence

of the receipt of the hash form from the client may be saved and noted, and the system may return to check if additional fields need processing.

[0119] FIG. 6 is a schematic diagram of a computer system 600. The system 600 can be used for the operations described in association with any of the computer-implement methods described previously, according to one implementation. The system 600 is intended to include various forms of digital computers, such as laptops, desktops, workstations, personal digital assistants, servers, blade servers, mainframes, and other appropriate computers. The system 600 can also include mobile devices, such as personal digital assistants, cellular telephones, smartphones, and other similar computing devices. Additionally the system can include portable storage media, such as, Universal Serial Bus (USB) flash drives. For example, the USB flash drives may store operating systems and other applications. The USB flash drives can include input/output components, such as a wireless transmitter or USB connector that may be inserted into a USB port of another computing device.

[0120] The system 600 includes a processor 610, a memory 620, a storage device 630, and an input/output device 640. Each of the components 610, 620, 630, and 640 are interconnected using a system bus 650. The processor 610 is capable of processing instructions for execution within the system 600. The processor may be designed using any of a number of architectures. For example, the processor 610 may be a CISC (Complex Instruction Set Computers) processor, a RISC (Reduced Instruction Set Computer) processor, or a MISC (Minimal Instruction Set Computer) processor.

[0121] In one implementation, the processor 610 is a single-threaded processor. In another implementation, the processor 610 is a multi-threaded processor. The processor 610 is capable of processing instructions stored in the memory 620 or on the storage device 630 to display graphical information for a user interface on the input/output device 640.

[0122] The memory 620 stores information within the system 600. In one implementation, the memory 620 is a computer-readable medium. In one implementation, the memory 620 is a volatile memory unit. In another implementation, the memory 620 is a non-volatile memory unit.

[0123] The storage device 630 is capable of providing mass storage for the system 600. In one implementation, the storage device 630 is a computer-readable medium. In various different implementations, the storage device 630 may be a floppy disk device, a hard disk device, an optical disk device, or a tape device.

[0124] The input/output device 640 provides input/output operations for the system 600. In one implementation, the input/output device 640 includes a keyboard and/or pointing device. In another implementation, the input/output device 640 includes a display unit for displaying graphical user interfaces.

[0125] The features described can be implemented in digital electronic circuitry, or in computer hardware, firmware, software, or in combinations of them. The apparatus can be implemented in a computer program product tangibly embodied in an information carrier, e.g., in a machine-readable storage device for execution by a programmable processor; and method steps can be performed by a programmable processor executing a program of instructions to perform functions of the described implementations by

operating on input data and generating output. The described features can be implemented advantageously in one or more computer programs that are executable on a programmable system including at least one programmable processor coupled to receive data and instructions from, and to transmit data and instructions to, a data storage system, at least one input device, and at least one output device. A computer program is a set of instructions that can be used, directly or indirectly, in a computer to perform a certain activity or bring about a certain result. A computer program can be written in any form of programming language, including compiled or interpreted languages, and it can be deployed in any form, including as a stand-alone program or as a module, component, subroutine, or other unit suitable for use in a computing environment.

[0126] Suitable processors for the execution of a program of instructions include, by way of example, both general and special purpose microprocessors, and the sole processor or one of multiple processors of any kind of computer. Generally, a processor will receive instructions and data from a read-only memory or a random access memory or both. The essential elements of a computer are a processor for executing instructions and one or more memories for storing instructions and data. Generally, a computer will also include, or be operatively coupled to communicate with, one or more mass storage devices for storing data files; such devices include magnetic disks, such as internal hard disks and removable disks; magneto-optical disks; and optical disks. Storage devices suitable for tangibly embodying computer program instructions and data include all forms of non-volatile memory, including by way of example semiconductor memory devices, such as EPROM, EEPROM, and flash memory devices; magnetic disks such as internal hard disks and removable disks; magneto-optical disks; and CD-ROM and DVD-ROM disks. The processor and the memory can be supplemented by, or incorporated in, ASICs (application-specific integrated circuits).

[0127] To provide for interaction with a user, the features can be implemented on a computer having a display device such as a CRT (cathode ray tube) or LCD (liquid crystal display) monitor for displaying information to the user and a keyboard and a pointing device such as a mouse or a trackball by which the user can provide input to the computer. Additionally, such activities can be implemented via touchscreen flat-panel displays and other appropriate mechanisms.

[0128] The features can be implemented in a computer system that includes a back-end component, such as a data server, or that includes a middleware component, such as an application server or an Internet server, or that includes a front-end component, such as a client computer having a graphical user interface or an Internet browser, or any combination of them. The components of the system can be connected by any form or medium of digital data communication such as a communication network. Examples of communication networks include a local area network (“LAN”), a wide area network (“WAN”), peer-to-peer networks (having ad-hoc or static members), grid computing infrastructures, and the Internet.

[0129] The computer system can include clients and servers. A client and server are generally remote from each other and typically interact through a network, such as the described one. The relationship of client and server arises by

virtue of computer programs running on the respective computers and having a client-server relationship to each other.

[0130] While this specification contains many specific implementation details, these should not be construed as limitations on the scope of any inventions or of what may be claimed, but rather as descriptions of features specific to particular implementations of particular inventions. Certain features that are described in this specification in the context of separate implementations can also be implemented in combination in a single implementation. Conversely, various features that are described in the context of a single implementation can also be implemented in multiple implementations separately or in any suitable subcombination. Moreover, although features may be described above as acting in certain combinations and even initially claimed as such, one or more features from a claimed combination can in some cases be excised from the combination, and the claimed combination may be directed to a subcombination or variation of a subcombination.

[0131] Similarly, while operations are depicted in the drawings in a particular order, this should not be understood as requiring that such operations be performed in the particular order shown or in sequential order, or that all illustrated operations be performed, to achieve desirable results. In certain circumstances, multitasking and parallel processing may be advantageous. Moreover, the separation of various system components in the implementations described above should not be understood as requiring such separation in all implementations, and it should be understood that the described program components and systems can generally be integrated together in a single software product or packaged into multiple software products.

[0132] Thus, particular implementations of the subject matter have been described. Other implementations are within the scope of the following claims. In some cases, the actions recited in the claims can be performed in a different order and still achieve desirable results. In addition, the processes depicted in the accompanying figures do not necessarily require the particular order shown, or sequential order, to achieve desirable results. In certain implementations, multitasking and parallel processing may be advantageous.

What is claimed is:

1. A computer-implemented method, comprising:
 - servicing, from a computer server system and to a plurality of different computing devices remote from the computer server system, web code that has been recoded to obscure its operation from malware that may be operating on the different computing devices;
 - receiving from different ones of the computing devices, an obfuscated representation of a particular parameter for a first of the computing devices, and a nonobfuscated representation of the same parameter for a second of the computing devices;
 - obfuscating the unobfuscated representation of the particular parameter, and comparing the obfuscated representation for the second of the computing devices with the obfuscated representation for the first of the computing devices; and
 - based on a determination that the obfuscated representations correspond to each other, correlating the obfuscated representation to the unobfuscated representation on the computer server system,

wherein the code for reporting parameters of the computing devices includes code for allowing the computing devices to determine whether to send an obfuscated representation or an unobfuscated representation.

2. The computer-implemented method of claim 1, wherein the code for allowing the computing devices to determine whether to send an obfuscated representation or an unobfuscated representation comprises biasing data that affects a frequency with which the computing devices select to send the plaintext representation or the hashed representation.

3. The computer-implemented method of claim 1, further comprising:

receiving from the computing devices, unobfuscated representations and obfuscated representations of a plurality of different parameters of the computing devices; obfuscating the received unobfuscated representations to created obfuscated values; and

using correlations between the obfuscated values and the received unobfuscated representations to identify parameters represented by the obfuscated representations.

4. The computer-implemented method of claim 1, further comprising using the obfuscated representation and the unobfuscated representation to identify characteristics of malware executing on the computing devices.

5. A computer-implemented method, comprising:

serving, from a computer server system and to a plurality of different computing devices remote from the computer server system, web code and code for reporting status of the computing devices;

receiving from one or more of the computing devices, first data that indicates a parameter of the one or more computing devices, the first data in a compressed format;

receiving from one or more others of the computing devices, second data that indicates the parameter of the one or more others of the computing devices, the second data in an uncompressed format; and

compressing the second data and comparing the compressed second data to the first data to correlate the first data to the second data,

wherein the code for reporting status of the computing devices includes code for allowing the computing devices to determine whether to send the first data or the second data.

6. The computer-implemented method of claim 5, wherein the code for allowing the computing devices to determine whether to send the first data or the second data comprises biasing data that affects a frequency with which the computing devices select to send the first data or the second data.

7. The computer-implemented method of claim 5, wherein the first data is compressed on the computing devices using hashing.

8. The computer-implemented method of claim 7, wherein the server system does not send hashing algorithm information to the computing devices.

9. The computer-implemented method of claim 5, further comprising using the compressed format to represent the parameter in identifying aggregate activity by multiple of the computing devices.

10. The computer-implemented method of claim 9, further comprising determining from the aggregate activity by

multiple of the computer devices whether ones of the multiple computing devices is infected with malware.

11. The computer-implemented method of claim 5, wherein the computer server system comprises an intermediary security server system that is separate from a web server system that generates and serves the web code.

12. The computer-implemented method of claim 5, further comprising comparing information sent with the compressed second data to information derived from the received first data to determine whether the compressed second data was generated from data that matches the first data.

13. One or more non-transitory storage devices storing instructions that, when executed by one or more computer processors, perform operations comprising:

serving, from a computer server system and to a plurality of different computing devices remote from the computer server system, web code and code for reporting status of the computing devices;

receiving from one or more of the computing devices, first data that indicates a parameter of the one or more computing devices, the first data in a compressed format;

receiving from one or more others of the computing devices, second data that indicates the parameter of the one or more others of the computing devices, the second data in an uncompressed format; and

compressing the second data and comparing the compressed second data to the first data to correlate the first data to the second data,

wherein the code for reporting status of the computing devices includes code for allowing the computing devices to determine whether to send the first data or the second data.

14. The one or more non-transitory storage devices of claim 13, wherein the code for allowing the computing devices to determine whether to send the first data or the second data comprises biasing data that affects a frequency with which the computing devices select to send the first data or the second data.

15. The one or more non-transitory storage devices of claim 13, wherein the first data is compressed on the computing devices using hashing.

16. The one or more non-transitory storage devices of claim 13, wherein the operations further comprise using the compressed format to represent the parameter in identifying aggregate activity by multiple of the computing devices.

17. The one or more non-transitory storage devices of claim 16, wherein the operations further comprise determining from the aggregate activity by multiple of the computer devices whether ones of the multiple computing devices is infected with malware.

18. The one or more non-transitory storage devices of claim 13, wherein the computer server system comprises an intermediary security server system that is separate from a web server system that generates and serves the web code.

19. The one or more non-transitory storage devices of claim 13, wherein the operations further comprise comparing information sent with the compressed second data to information derived from the received first data to determine whether the compressed second data was generated from data that matches the first data.