

(51) International Patent Classification:

H04L 9/32 (2006.01)

G06F 21/00 (2013.01)

H04L 29/06 (2006.01)

H04L 9/14 (2006.01)

(21) International Application Number:

PCT/US2019/035737

(22) International Filing Date:

06 June 2019 (06.06.2019)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

62/682,337

08 June 2018 (08.06.2018)

US

(71) Applicant: JPMORGAN CHASE BANK, N.A. [US/US];
383 Madison Avenue, New York, NY 10179 (US).

(72) Inventors: SUNDAR, Gayathri; 383 Madison Avenue,
New York, NY 10179 (US). HAGUE, Jeffrey; 383 Madison
Avenue, New York, NY 10179 (US).

(74) Agent: SONG, Yisun et al.; Hunton Andrews Kurth LLP,
2200 Pennsylvania Ave, NW, Washington, DC 20037 (US).

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

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ,
UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,
TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,
EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

(54) Title: SYSTEM AND METHOD FOR MULTI-CERTIFICATE PINNING

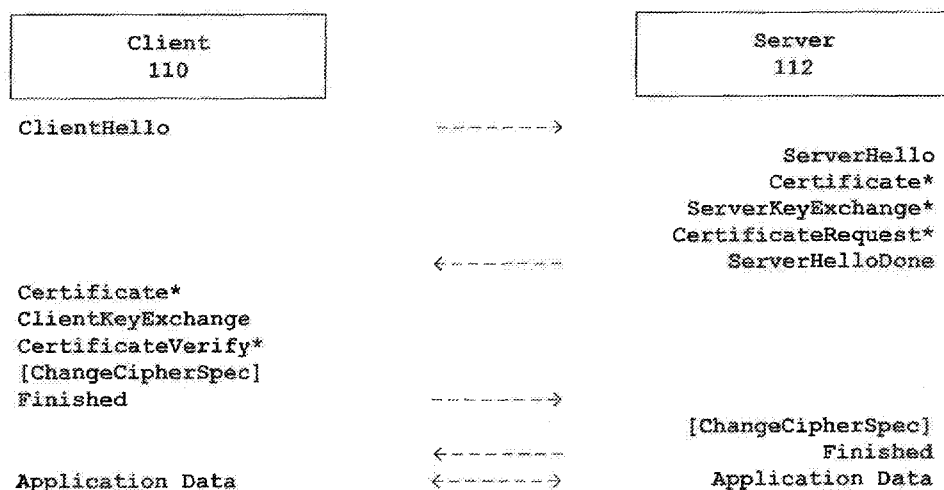


Figure 1

(57) Abstract: An embodiment of the present invention is directed to a multi-certificate pinning. The innovative system configures servers with at least two certificates from multiple different vendors/sources with differing expiration dates. This provides lead time to replace voided/expired certificates. If a first certificate expires, the system uses another valid certificate for that server until the certificated is addressed, thereby avoiding service down times. Accordingly, providers are not required to expedite mobile app store submission.



TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

Published:

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

SYSTEM AND METHOD FOR MULTI-CERTIFICATE PINNING

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] The application claims priority to U.S. Provisional Application 62/682,337 (Attorney Docket No. 72167.001436), filed June 8, 2018, the contents of which are incorporated herein in its entirety.

FIELD OF THE INVENTION

[0002] The invention relates generally to a system and method for implementing multi-certificate pinning with multiple certificates having different expiration times.

BACKGROUND OF THE INVENTION

[0003] Certificate pinning with a single certificate has issues with respect to outages caused by certificate expirations on servers. The single certificate is often also baked into the mobile application sandbox which requires a repackaging of the mobile app with a new certificate and a resubmission to app stores. When the certificate expires, service may be disrupted until the certificate is renewed. On the server side, certificates need to be renewed on time and overlap properly to avoid outages and disruptions in service.

[0004] These and other drawbacks exist.

SUMMARY OF THE INVENTION

[0005] According to one embodiment, the invention relates to a mobile device system that implements multi-certificate pinning. A mobile device comprises: a memory component; a network communication interface that is in communication with a remote server such as a content delivery network; and a microprocessor, coupled to the memory component and the network communication interface, the microprocessor configured to perform the steps of:

requesting a first certificate and a second certificate from the remote server, wherein the first certificate has a first expiration and the second certificate has a second expiration different from the first expiration; executing an application on the mobile device by using the first certificate to make a connection to the server; and prior to or upon an expiration of the first certificate, switching to the second certificate wherein the application now uses the second certificate to make the connection to the remote server.

[0006] According to another embodiment, the invention relates to a mobile device system that implements multi-certificate pinning. A mobile device comprises: a memory component; a network communication interface that is in communication with a remote server such as a content delivery network; and a microprocessor, coupled to the memory component and the network communication interface, the microprocessor configured to perform the steps of: requesting and receiving a first certificate; requesting and receiving a second certificate in advance of an expiration of the first certificate; updating at least one application executing on the mobile device to contain the first certificate and the second certificate; requesting and receiving a third certificate in advance of the expiration of the first certificate; and upon expiration of the first certificate; updating the at least one application executing on the mobile device to contain the second certificate and the third certificate.

[0007] According to another embodiment, the invention relates to a method that implements multi-certificate pinning. A method comprises the steps of: requesting a first certificate and a second certificate from a remote server such as a content delivery network, wherein the first certificate has a first expiration and the second certificate has a second expiration different from the first expiration; executing an application on a mobile device by using the first certificate to make a connection to a server; and prior to or upon an expiration of

the first certificate, switching to the second certificate wherein the application now uses the second certificate to make the connection to the remote server.

[0008] The mobile device may include a specially programmed computer system comprising one or more computer processors, electronic storage devices, and networks.

[0009] The computer implemented mobile device system, method and medium described herein provide unique advantages to entities, organizations, mobile device users, application developers and providers, and various other users, according to various embodiments of the invention. The innovative mobile device system mitigates risks by having multiple pins associated with a server. Specifically, a host service may supply the pins to ensure at any given time, there is at least one valid pin stored by a mobile application, including a mobile Software Development Kit (SDK), thus preventing Denial of Service (DOS). The innovative methodology provides sufficient time to update an expired or breached certificate on a remote server such as a Content Delivery Network (CDN) as well as within a SDK/mobile application. If one particular certificate authority (CA) is compromised, having two different CA issued server certificates would immediately suspend a breached certificate, thereby achieving improved resiliency. These and other advantages will be described more fully in the following detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] In order to facilitate a fuller understanding of the present invention, reference is now made to the attached drawings. The drawings should not be construed as limiting the present invention, but are intended only to illustrate different aspects and embodiments of the invention.

[0011] Figure 1 is an exemplary message flow for a full handshake.

[0012] Figure 2 is an exemplary dynamic certification pinning session, according to an embodiment of the present invention.

[0013] Figure 3 is an exemplary multi-certificate pinning approach, according to an embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT(S)

[0014] The following description is intended to convey an understanding of the present invention by providing specific embodiments and details. It is understood, however, that the present invention is not limited to these specific embodiments and details, which are exemplary only. It is further understood that one possessing ordinary skill in the art, in light of known systems and methods, would appreciate the use of the invention for its intended purposes and benefits in any number of alternative embodiments, depending upon specific design and other needs.

[0015] An embodiment of the present invention is directed to configuring servers with multiple certificates from multiple different vendors/sources with differing expiration dates. According to an embodiment of the present invention, a server may be configured with multiple certificates. For example, a server may be configured with two certificates where each certificate is from a different provider. This provides lead time to replace voided and/or expired certificates as well as address other issues. For example, if a first certificate expires, the system may use another valid certificate for that server until the certificate renewal is addressed, thereby avoiding service down times. Accordingly, providers are not required to expedite mobile app store submission.

[0016] Figure 1 is an exemplary message flow for a full handshake between Client 110 and Server 112. Transport Layer Security (TLS) may be classified into a TLS handshake

protocol and a TLS record protocol. As shown in Figure 1, there are two parts to securing application data that is going out on the wire/over the air (OTA). An exemplary scenario may use a symmetric cipher (*e.g.*, AES/3DES/RC4, *etc.*) to encrypt data carried by the TLS record protocol owing to its properties of speed and scalability. In order to achieve this, an authenticated trusted tunnel may be established between two negotiating parties to exchange secrets that would end up deriving the same symmetric keys on both sides, without actually sending it out on the wire/OTA. The TLS Handshake protocol provides this. As part of establishing this trust, asymmetric ciphers, such as RSA, DH and ECC, may be used.

[0017] With regards to RSA/DH *etc.*, a key pair may be derived such that given a public counterpart, it would be computationally infeasible to derive its private counterpart given current resource capabilities. Such hurdles may include addressing computationally difficult problems such as factoring of large primes, discrete logarithms, *etc.* The public key may be broadcast and a corresponding private key may be secured. These algorithms may be designed in a way that the traffic is encrypted with the public key and decrypted with its corresponding private key.

[0018] Given this background, the TLS Handshake protocol may mandate server authentication and optionally client authentication. There is an optional third mode called Anonymous TLS, where neither party is authenticated by a trusted certificate. Accordingly, certificate pinning does not apply there.

[0019] Because the server certificate is mandated, an embodiment of the present invention may rely on trusting the received certificate which vouches for its public key. Keying material may be exchanged by encrypting the data with a peer's public key. Accordingly, validating the public key as belonging to its owner is crucial in establishing trust as part of the TLS Handshake protocol.

[0020] Currently, mobile applications statically pin certificates that are needed to be validated (*e.g.*, service endpoints that they consume, *etc.*). This is not a truly scalable solution as it requires providers to constantly validate the correctness of these certificates manually prior to release cycles. In addition, current systems require dependency on various third party owned applications which consume SDKs to rollout an update as soon as pins either expire or experience a breach that needs to be quickly acted upon.

[0021] An embodiment of the present invention is directed to a dynamic certificate pinning framework to address these concerns where pins are hosted on a site, (*e.g.*, public site) which may be accessible from various environments. For example, pins may be hosted on a CDN, which may be dynamically pulled and updated at run time.

[0022] Although this addresses an issue of getting pins on the fly for various servers that are consumed from mobile applications, a first connection to CDN itself may be statically pinned, and again bundled as part of a third party SDK application to ensure Trust on First Use (TOFU). Under this scenario, third party applications have a version of a SDK that could potentially have an expired Static pin of CDN, which would cause a denial of service. For example, some third parties are not willing (or simply fail) to update SDK for long periods of time, *e.g.*, months, years, *etc.* Oftentimes, terms and conditions with third parties do not force them to upgrade right away but within a period of at least a predetermined number of months (*e.g.*, 6 months, *etc.*) to take a newer version of the SDK.

[0023] An embodiment of the present invention is directed to ensuring enough lead time to update expired certificates and/or change certificates as part of certificate rotation policies and ensure functionality does not break within mobile applications that are in market. An embodiment of the present invention is directed to executing multiple valid certificates on

servers such that they are out of sync by a predetermined time period (*e.g.*, few months, weeks, days, *etc.*) in terms of their validity. This ensures that at any given time, one valid pin is available for any given server.

[0024] This certificate pattern is further useful when it comes to Frameworks that may be distributed to third party merchant applications. For example, a provider may depend on vendors updating their application with pins as the provider now may become a third party from their context. In this example, a financial institution may provide frameworks to merchants, *e.g.*, a Mobile Pay SDK, which has pins baked into it for requesting banking and payment services. This may be abstracted from a Merchant perspective. In addition, different certificate authorities (CAs) issuing different certificates to the same server may further provide improved resiliency. Within the context of the various features of an embodiment of the present invention, pins and certificates may be used interchangeably.

[0025] An embodiment of the present invention is directed to preventing denial of service (DOS) based on pins expiration where the system is ensured to have at least one valid pin in operation. The system further avoids the need to push for new SDK versions to already integrated third parties as the CDN itself may host its own new pins, which may be fetched using the other valid pin and overwritten within the SDK. The system further effectuates improved resiliency as the system has access to more than one trusted CA issued server certificate configured on the system.

[0026] The various embodiments of the present invention may be applied to different scenarios. For example, a Merchant SDK may be distributed to various vendors with dynamic certificate pinning. Also, multiple valid pins configured against servers may prevent DOS until certificates are updated. Any system that mobile applications hit/access may implement

certificate pinning. In addition, upgrades to dynamic certificate pinning framework may implement these features. An embodiment of the present invention is directed to configuring a server hosting the pins to have at least two different certificates issued by different CAs, at varying expiration dates and/or conditions.

[0027] According to an exemplary embodiment, dynamic certificate pinning may be applied to a Merchant SDK. In this application, the Merchant SDK may be bundled with two certificates. An intermediate certificate of CDN may host the certificates that the Merchant SDK may need to hit AUTH and gateway (GWO). A root CDN certificate may be used for a single time failover scenario. For the failover scenario, intermediates of AUTH/GWO may be bundled as well. In this example, the Merchant SDK may consume two frameworks: a Certificate Pinning Framework and a Sync Manager Framework. The Certificate Pinning Framework may manage the certificate pinning requirements on a network connection and validate if the connection is pinned against a valid certificate or not. The Sync Manager Framework may fetch the latest pins from CDN when requested by the Merchant SDK.

[0028] The Merchant SDK may load intermediate certificates (*e.g.*, CDN, AUTH and GWO) from its bundle into a documents folder/certificates or other dedicated space within an app to persist the certificates. After the initial loading, the Merchant SDK may directly load from the documents folder/certificates and set into the Certificate Pinning Framework. The Merchant SDK may attempt a connection to AUTH and GWO in a BAU flow. If the Certificate Pinning Framework returns an error, a sync may be applied to connect to the CDN with the persisted Intermediate certificate of CDN that was previously set. If the connection to CDN succeeds, the latest pins of AUTH, GWO and CDN may be downloaded and the documents folder/certificates may be overwritten.

[0029] If the connection to CDN with the Intermediate CDN certificate fails, a failover scenario may be initiated to recover and prevent DOS. In accordance with an embodiment of the present invention, two different intermediate certificates for CDN with varying expiration times, offset by a predetermined time period (*e.g.*, 6 months, *etc.*) may rotate the expired certificate so that there is enough lead time to replace the pin on CDN. In this example, the system may not need to failover to a root certificate and accordingly, a connection to CDN may be pinned to prevent interruption. In this scenario, when a fetch from CDN is successful and the pins within the SDK are overwritten, the system should have valid certificates so that a sync manager does not need to be called.

[0030] Figure 2 is an exemplary dynamic certificate pinning approach, according to an embodiment of the present invention. As shown in Figure 2, an embodiment of the present invention may configure servers with at least two pins obtained from different CAs with differing validity periods so that at any given time one of them is valid.

[0031] Figure 2 illustrates interactions between and among Device 210, Content Delivery Network (CDN) 212 and Server 214. Device 210 may represent any mobile device, *e.g.*, smart phone, tablet, computer, laptop, portable device, wearable, terminal, kiosk, *etc.* Device 210 may represent any client device that communicates with a server. Device 210 may execute an application (“app”) or other software program. According to another example, Devices 210 may represent various consumer devices including IoT devices, smart home devices, speakers, personal assistant devices, wearables, smart vehicles, *etc.* Device 210 may represent a plurality of devices, network of devices, aggregated devices, *etc.* For example, a smart home may include multiple home devices, *e.g.*, home security, appliances, furniture, electronics, personal assistant device, *etc.* that may communicate with a hub device. The hub device may then communicate

with CDN 212 and Server 214. In this example, the hub device may further manage the certificates. Other scenarios and applications may be implemented in accordance with the embodiments of the present invention. Devices 210 may also represent any device that executes an application or other software program.

[0032] CDN 212 may represent a content delivery network or remote server that may be hosted by a service provider, third party, and/or other entity. For example, the application executing on the device and the CDN may be part of the same entity. In the example of Figure 2, CDN 212 may manage pins and certificates. For example, CDN 212 may maintain a copy of some or all the certificates on behalf of the systems that the application is communicating with. Server 214 may represent a gateway, a router, or a node in a computer network. For example, Server 214 may represent a payment gateway or other communication or transaction gateway or server. While Figure 2 shows a single component for illustration, multiple components may be supported.

[0033] As shown in Figure 2, Device 210 may request pins from CDN 212, at 220. In response, pins of backend systems and CDN pins may be transmitted to Device 210, as shown by 222. Pins may persist on Software Development Kit (SDK), at 224. A pinned connection to Server 214 may be established at 226. A response indicating success may be provided at 228 to Device 210. At 230, pin 2 may be determined to be invalid. Pin 2 may be updated on CDN 212, at 232. At 234, pin 2 may be updated on the SDK. As shown in Figure 2, if a pin becomes invalid, a second valid pin may be used. The first pin may then be renewed or restored to a valid state. The order illustrated in Figure 2 is merely exemplary. While the process of Figure 2 illustrates certain steps performed in a particular order, it should be understood that the embodiments of the present invention may be practiced by adding one or more steps to the

processes, omitting steps within the processes and/or altering the order in which one or more steps are performed.

[0034] Figure 3 is an exemplary multi-certificate pinning approach, according to an embodiment of the present invention. Certificates (Certs) may be created at predetermined intervals, *e.g.*, every 6 months, for 1 of 2 valid web service URLs, that are valid for a term, *e.g.*, 1 year. Mobile apps may then pin the two currently valid certs. URL examples may include: mobile.bankABC.com and mobile-new.bankABC.com. The example of Figure 3 shows two URLs. However, additional URLs may be applied in accordance with the embodiments of the present invention.

[0035] Certificate pinning may be performed at a leaf in order to provide protection against certificate authority (CA) compromise. For example, certificates may be chained. More specifically, certificates may be issued by a root CA, with multiple intermediaries. A leaf certificate may be an actual server certificate, issued to the particular server. For example, a leaf certificate may represent an end-entity or last certificate in a chain. An embodiment of the present invention may technically pin against any certificate within the chain. In this context, the lower in chain represents better security. Web traffic may continue to use the existing URLs as there is no certificate pinning impact.

[0036] In the example of Figure 3, applications (apps) may try URL 1 first. If URL 1 fails, then apps may use URL 2. To avoid extra traffic, the app may store the latest successful URL and use it until it no longer works. Figure 3 illustrates an example of two URLs. Other additional URLs may be implemented in accordance with the various embodiments of the present invention.

[0037] Figure 3 illustrates Current/Startup timeline 310 and Business as Usual (BAU) timeline 312. For URL 1 and URL 2, a sequence of certificates may be applied in a manner that ensures business as usual operations. At 320, Cert 2 may be created. Cert 2 may be created a predetermined number of days in advance, *e.g.*, 30 days in advance. At 322, applications may be updated to contain Cert 1 and Cert 2 hashes. Cert 3 may be created a predetermined number of days in advance, *e.g.*, 30 days in advance. Prior to Cert 1 expiring, a forced upgrade may be applied at 324. Upon Cert 1 expiring, applications may be updated to contain Cert 2 and Cert 3 hashes, at 326. Cert 4 may be created a predetermined number of days in advance, *e.g.*, 30 days in advance. Prior to Cert 2 expiring, a forced upgrade may be applied at 328. Upon Cert 2 expiring, applications may be updated to contain Cert 3 and Cert 4 hashes, at 330.

[0038] Cert 5 may be created a predetermined number of days in advance, *e.g.*, 30 days in advance. Prior to Cert 3 expiring, a forced upgrade may be applied at 332. Upon Cert 3 expiring, applications may be updated to contain Cert 4 and Cert 5 hashes, at 334. Cert 6 may be created a predetermined number of days in advance, *e.g.*, 30 days in advance. Prior to Cert 5 expiring, a forced upgrade may be applied at 336. Upon Cert 5 expiring, applications may be updated to contain Cert 5 and Cert 6 hashes, at 338. The process may continue.

[0039] The foregoing examples show the various embodiments of the invention in one physical configuration; however, it is to be appreciated that the various components may be located at distant portions of a distributed network, such as a local area network, a wide area network, a telecommunications network, an intranet and/or the Internet. Thus, it should be appreciated that the components of the various embodiments may be combined into one or more devices, collocated on a particular node of a distributed network, or distributed at various locations in a network, for example. As will be appreciated by those skilled in the art, the

components of the various embodiments may be arranged at any location or locations within a distributed network without affecting the operation of the respective system.

[0040] As described above, the various embodiments of the present invention support a number of communication devices and components, each of which may include at least one programmed processor and at least one memory or storage device. The memory may store a set of instructions. The instructions may be either permanently or temporarily stored in the memory or memories of the processor. The set of instructions may include various instructions that perform a particular task or tasks, such as those tasks described above. Such a set of instructions for performing a particular task may be characterized as a program, software program, software application, app, or software.

[0041] It is appreciated that in order to practice the methods of the embodiments as described above, it is not necessary that the processors and/or the memories be physically located in the same geographical place. That is, each of the processors and the memories used in exemplary embodiments of the invention may be located in geographically distinct locations and connected so as to communicate in any suitable manner. Additionally, it is appreciated that each of the processor and/or the memory may be composed of different physical pieces of equipment. Accordingly, it is not necessary that the processor be one single piece of equipment in one location and that the memory be another single piece of equipment in another location. That is, it is contemplated that the processor may be two or more pieces of equipment in two or more different physical locations. The two distinct pieces of equipment may be connected in any suitable manner. Additionally, the memory may include two or more portions of memory in two or more physical locations.

[0042] As described above, a set of instructions is used in the processing of various embodiments of the invention. The servers may include software or computer programs stored in the memory (*e.g.*, non-transitory computer readable medium containing program code instructions executed by the processor) for executing the methods described herein. The set of instructions may be in the form of a program or software or app. The software may be in the form of system software or application software, for example. The software might also be in the form of a collection of separate programs, a program module within a larger program, or a portion of a program module, for example. The software used might also include modular programming in the form of object oriented programming. The software tells the processor what to do with the data being processed.

[0043] Further, it is appreciated that the instructions or set of instructions used in the implementation and operation of the invention may be in a suitable form such that the processor may read the instructions. For example, the instructions that form a program may be in the form of a suitable programming language, which is converted to machine language or object code to allow the processor or processors to read the instructions. That is, written lines of programming code or source code, in a particular programming language, are converted to machine language using a compiler, assembler or interpreter. The machine language is binary coded machine instructions that are specific to a particular type of processor, *i.e.*, to a particular type of computer, for example. Any suitable programming language may be used in accordance with the various embodiments of the invention. For example, the programming language used may include assembly language, Ada, APL, Basic, C, C++, COBOL, dBase, Forth, Fortran, Java, Modula-2, Pascal, Prolog, REXX, Visual Basic, JavaScript, Objective-C, Swift, Kotlin and/or Python. Further, it is not necessary that a single type of instructions or single programming

language be utilized in conjunction with the operation of the system and method of the invention. Rather, any number of different programming languages may be utilized as is necessary or desirable.

[0044] Also, the instructions and/or data used in the practice of various embodiments of the invention may utilize any compression, obfuscation or encryption technique or algorithm, as may be desired. An encryption module might be used to encrypt data. Further, files or other data may be decrypted using a suitable decryption module, for example.

[0045] In the system and method of exemplary embodiments of the invention, a variety of “user interfaces” may be utilized to allow a user to interface with the mobile devices or other personal computing device. As used herein, a user interface may include any hardware, software, or combination of hardware and software used by the processor that allows a user to interact with the processor of the communication device. A user interface may be in the form of a dialogue screen provided by an app, for example. A user interface may also include any of touch screen, keyboard, voice reader, voice recognizer, dialogue screen, menu box, list, checkbox, toggle switch, a pushbutton, a virtual environment (*e.g.*, Virtual Machine (VM)/cloud), or any other device that allows a user to receive information regarding the operation of the processor as it processes a set of instructions and/or provide the processor with information. Accordingly, the user interface may be any system that provides communication between a user and a processor. The information provided by the user to the processor through the user interface may be in the form of a command, a selection of data, or some other input, for example.

[0046] The software, hardware and services described herein may be provided utilizing one or more cloud service models, such as Software-as-a-Service (SaaS), Platform-as-a-Service

(PaaS), and Infrastructure-as-a-Service (IaaS), and/or using one or more deployment models such as public cloud, private cloud, hybrid cloud, and/or community cloud models.

[0047] Although the embodiments of the present invention have been described herein in the context of a particular implementation in a particular environment for a particular purpose, those skilled in the art will recognize that its usefulness is not limited thereto and that the embodiments of the present invention can be beneficially implemented in other related environments for similar purposes.

WHAT IS CLAIMED IS:

1. A mobile device that implements multi-certificate pinning, the mobile device comprising:

a memory component;

a network communication interface that is in communication with a remote server; and

a microprocessor, coupled to the memory component and the network communication interface, the microprocessor configured to perform the steps of:

requesting a first certificate and a second certificate from the remote server, wherein the first certificate has a first expiration and the second certificate has a second expiration different from the first expiration;

executing an application on the mobile device by using the first certificate to make a connection to the server; and

prior to or upon an expiration of the first certificate, switching to the second certificate wherein the application now uses the second certificate to make the connection to the remote server.

2. The mobile device of claim 1, wherein the microprocessor is further configured to perform the step of:

renewing the first certificate to a valid state.

3. The mobile device of claim 1, wherein the microprocessor is further configured to perform the step of:

updating the application to contain a first certificate hash and a second certificate hash.

4. The mobile device of claim 1, wherein the microprocessor is further configured to perform the step of:

creating a third certificate in advance to the expiration of the first certificate.

5. The mobile device of claim 1, wherein the first certificate corresponds to a first URL.

6. The mobile device of claim 1, wherein the second certificate corresponds to a second URL.

7. The mobile device of claim 1, wherein the mobile device comprises an Internet of Things (IoT) device.

8. A mobile device that implements multi-certificate pinning, the mobile device comprising:

a memory component;

a network communication interface that is in communication with a remote server; and

a microprocessor, coupled to the memory component and the network communication interface, the microprocessor configured to perform the steps of:

requesting a first certificate;

receiving a second certificate in advance of an expiration of the first certificate;

updating at least one application executing on the mobile device to contain the first

certificate and the second certificate;

receiving a third certificate in advance of the expiration of the first certificate; and

upon expiration of the first certificate; updating the at least one application executing on the mobile device to contain the second certificate and the third certificate.

9. The mobile device of claim 8, wherein the microprocessor is further configured to perform the step of:

renewing the first certificate to a valid state.

10. The mobile device of claim 8, wherein the microprocessor is further configured to perform the step of:

updating the application to contain a first certificate hash and a second certificate hash.

11. The mobile device of claim 8, wherein the microprocessor is further configured to perform the step of:

creating a fourth certificate in advance to the expiration of the first certificate.

12. The mobile device of claim 8, wherein the first certificate corresponds to a first URL.

13. The mobile device of claim 8, wherein the second certificate corresponds to a second URL.

14. The mobile device of claim 8, wherein the mobile device comprises an Internet of Things (IoT) device.

15. A method that implements multi-certificate pinning, the method comprising the steps of:

requesting a first certificate and a second certificate from a remote server, wherein the first certificate has a first expiration and the second certificate has a second expiration different from the first expiration;

executing an application on a mobile device by using the first certificate to make a connection to a server; and

prior to or upon an expiration of the first certificate, switching to the second certificate wherein the application now uses the second certificate to make the connection to the remote server.

16. The method of claim 15, further comprising the step of:
renewing the first certificate to a valid state.

17. The method of claim 15, further comprising the step of:
updating the application to contain a first certificate hash and a second certificate hash.

18. The method of claim 15, further comprising the step of:
creating a third certificate in advance to the expiration of the first certificate.

19. The method of claim 15, wherein the first certificate corresponds to a first URL.
20. The method of claim 15, wherein the second certificate corresponds to a second URL.

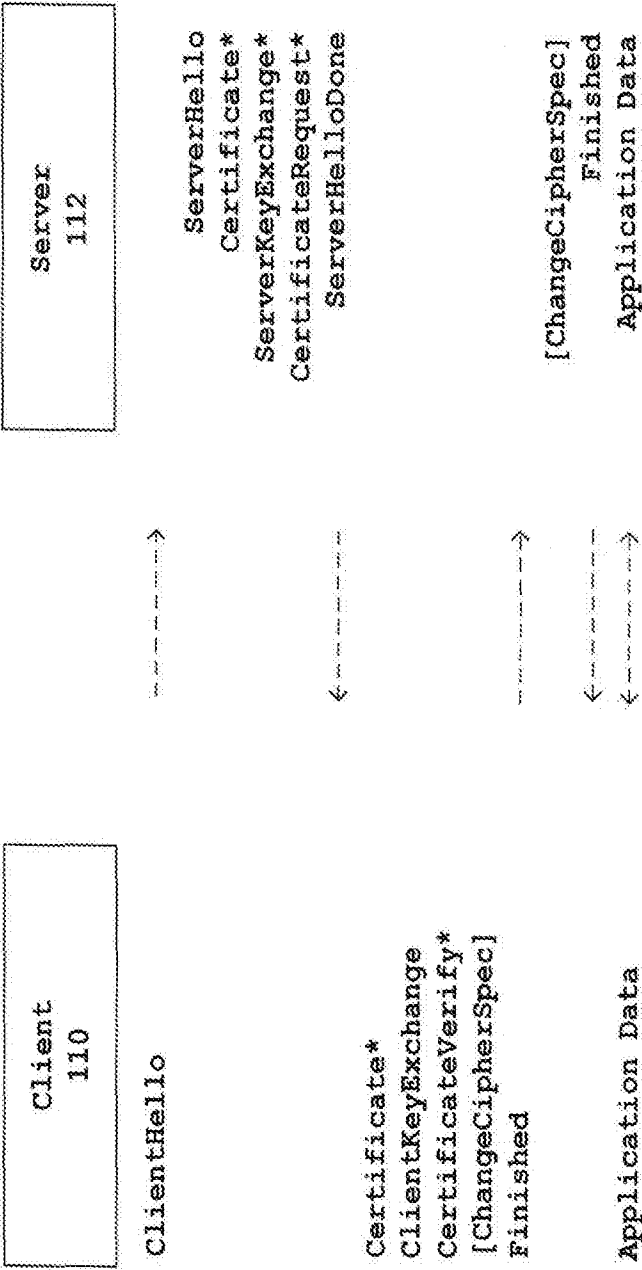


Figure 1

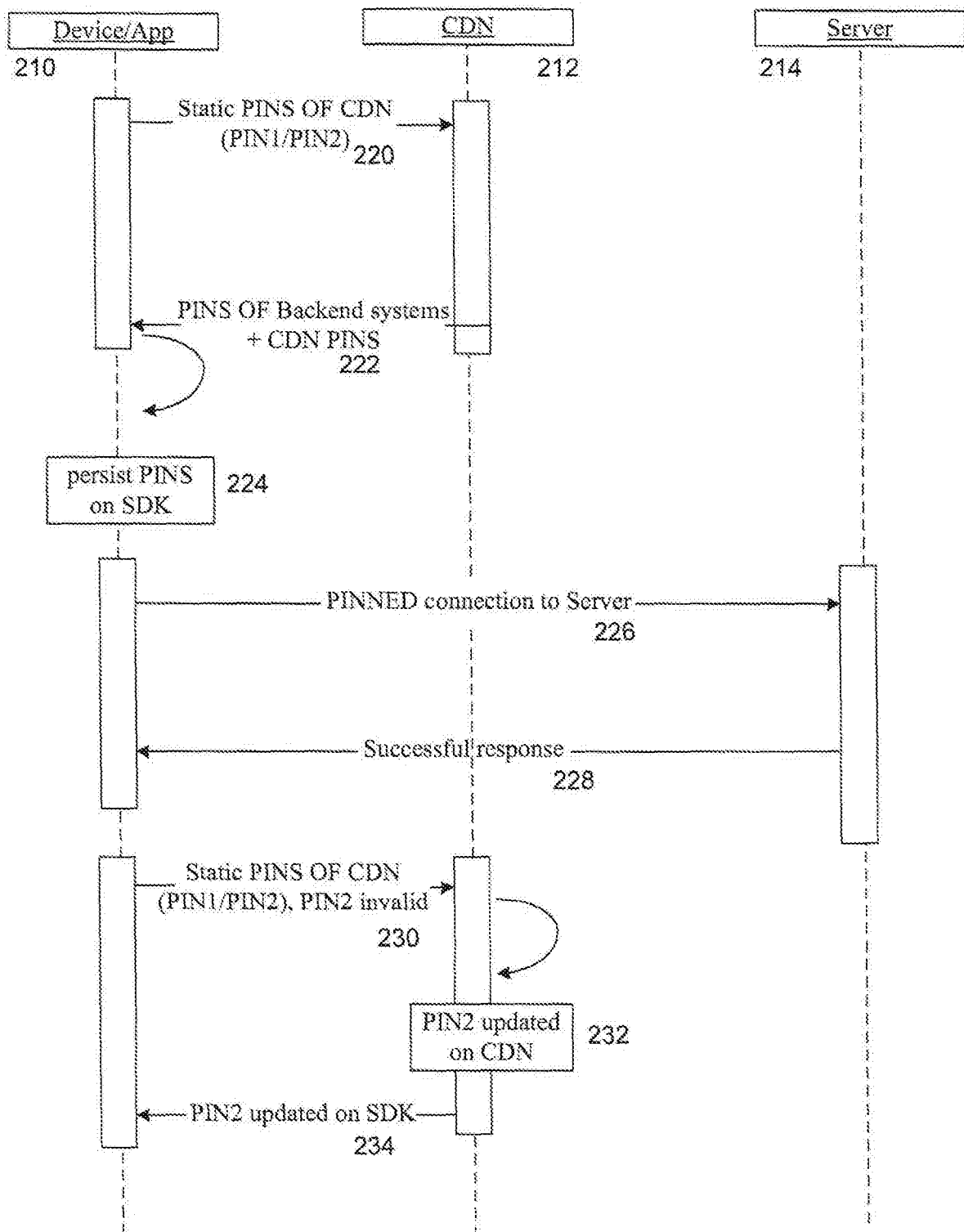


Figure 2

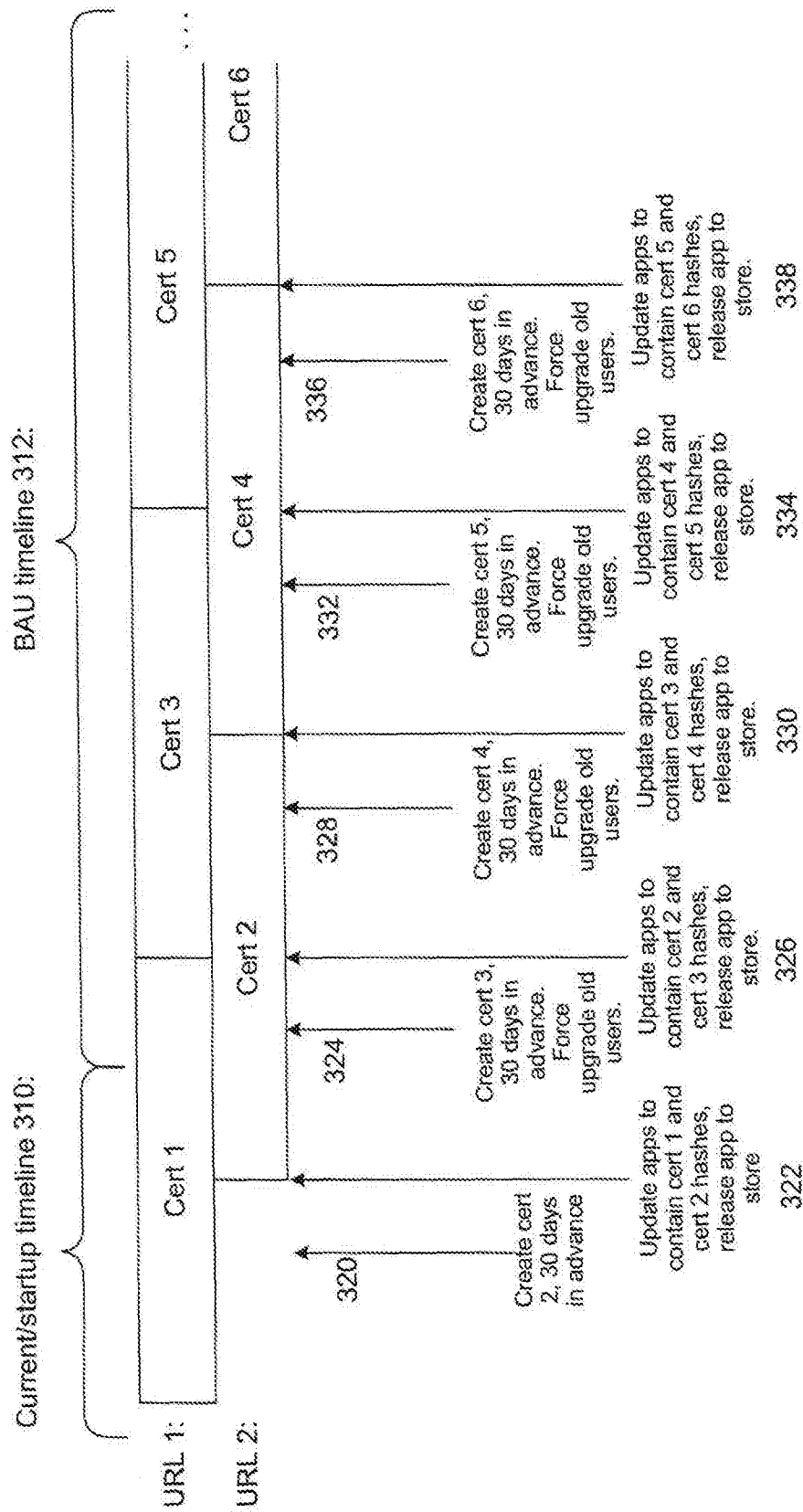


Figure 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US2019/035737

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - H04L 9/32; H04L 29/06; G06F 21/00; H04L 9/14 (2019.01)

CPC - H04L 63/0823; H04L 9/3268; G06F 21/33; H04L 9/3265 (2019.05)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

See Search History document

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

USPC - 713/155; 713/156; 713/157; 713/158 (keyword delimited)

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

See Search History document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2017/0230355 A1 (CITRIX SYSTEMS, INC.) 10 August 2017 (10.08.2017) entire document	1, 5-7, 15, 19, 20
---		---
Y		2-4, 8-14, 16-18
Y	US 2017/0171191 A1 (AMAZON TECHNOLOGIES, INC.) 15 June 2017 (15.06.2017) entire document	2, 9, 16
Y	EP 3232640 A1 (BUNDESDRUCKEREI GMBH) 18 October 2017 (18.10.2017) entire document	3, 4, 8-14, 17, 18
A	US 2011/0154027 A1 (LIU et al) 23 June 2011 (23.06.2011) entire document	1-20
A	US 2004/0148505 A1 (QIU) 29 July 2004 (29.07.2004) entire document	1-20
A	US 2013/0227275 A1 (SATO) 29 August 2013 (29.08.2013) entire document	1-20

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

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

01 August 2019

Date of mailing of the international search report

20 AUG 2019

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, VA 22313-1450
Facsimile No. 571-273-8300

Authorized officer

Blaine R. Copenheaver

PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774