

METHOD AND SYSTEM FOR HYPERVISOR-BASED ATTESTATION OF DATA PROVENANCE

Field of Invention

The invention relates to methods and systems for securing communication
5 between a client mobile device and a remote server, and more particularly to using
hypervisor in such methods and systems.

Background

Due to growing popularity of smart phones and the rapid development of
mobile internet, there is an increased number of malware targeting smart phones.
10 Attackers may inject rootkits on the mobile phone to compromise the operating
system. An intelligent rootkit may capture user credentials and impersonate a
human user (victim). For instance, a keylogger is capable of capturing a user
password and logging into an online banking server; it is also capable of sending a
large number of MMS without the human user's notice. Accordingly, mobile
15 security is imperative.

Many existing security solutions are available, but have their drawbacks.

ARM's (ARM Holdings) TrustZone security framework partitions hardware
and software resources into the Secure World and the Normal World. As such,
resources in the Secure World, such as registers and memory segments, cannot
20 be accessed by software in the Normal World, whereas the resources in the
Normal World can be accessed by software in the Secure World. Accordingly, the
Secure World is secured against attacks from the Normal World, but is not secured
against attacks within the Secure World. When an Android application runs in the

Secure World, security is still dependent on the underlying operating system, libraries and middleware in the same Secure World. In other words, the trusted computing base (TCB) in TrustZone-based systems is typically large thereby weakening the security.

5 Further, most ARM chip manufacturers do not allow a software to utilize the TrustZone extension without prior authorization. In order to run an application in the Secure World, the software is required to be signed by the vendor. The hardware verifies the signature before loading the code. Although this imposes a restriction on the application developer, the manufacturer's signature or
10 authorization does not guarantee the signed code is benign.

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) verifies whether data is sent in a human user's presence. It is widely used to prevent malware from automatically executing a transaction, e.g., a password submission. Typically, CAPTCHA challenges require human intelligence
15 to solve, e.g., to visually recognize characters or evaluate an equation presented in a distorted image. However, in recent years, commonly used CAPTCHA challenges have been circumvented by automated attacks. A strong CAPTCHA scheme incurs a heavy performance toll on the verifier, as the verifier has to prepare a large database with well-designed challenges. CAPTCHA also cannot
20 cope with a malicious human user who impersonates the victim.

Summary

Embodiments of the invention improve mobile security in communication between client mobile device and remote server through hypervisor-based attestation of data provenance. The invention provides a solution for differentiating

between software user and hardware or human user, a second factor for authentication even in a situation of compromised user credential, and/or a non-repudiating evidence for transaction authorisation.

According to one embodiment of the invention, a method implementable at a mobile device for attestation of data provenance, comprises: in response to a request to authenticate a user to a remote server via a client application which resides in the mobile device, performing the following by a hypervisor: clearing a buffer and blocking write permission of software on the buffer, intercepting an interrupt which is generated after raw data is written into the buffer, and transferring the raw data from the buffer to the hypervisor, unblocking write permission of software on the buffer, signing the raw data with a security information which at least includes a hypervisor signature and a current timestamp, for generating a current attestation message; and submitting the current attestation message to the remote server, wherein if a valid signature signed with any raw data is to be detected present in the current attestation message, and if an identical precedent for the current timestamp is to be detected absent from any previous attestation message for a user identity of the current attestation message, data provenance as from authenticated human user is to be ascertained at the remote server, and wherein if a valid hypervisor signature signed with any raw data is to be detected absent in the current attestation message, data provenance as from software user is to be ascertained at the remote server.

According to one embodiment of the invention, a method implementable at a server for attestation of data provenance, comprises: receiving a current attestation message; detecting a presence or an absence of a valid hypervisor signature signed with any raw data in the current attestation message; detecting a

presence or an absence of an identical precedent for a current timestamp included in the current attestation message from any previous attestation message for a user identity of the current attestation message; if a presence of a valid signature signed with any raw data is detected in the current attestation message, and if an
5 absence of an identical precedent of the current timestamp is detected, ascertaining data provenance as from authenticated human user; and if an absence of a valid hypervisor signature signed with any raw data is detected in the current attestation message, ascertaining data provenance as from software user.

According to one embodiment of the invention, a method for attestation of
10 data provenance, comprises: in response to a request to authenticate a user to a remote server via a client application which resides in a mobile device, performing the following by a hypervisor: clearing a buffer and blocking write permission of software on the buffer, intercepting an interrupt which is generated after raw data is written into the buffer, and transferring the raw data from the buffer to the
15 hypervisor, unblocking write permission of software on the buffer, and signing the raw data with a security information which at least includes a hypervisor signature and a current timestamp for generating a current attestation message; submitting the attestation message to the remote server; and at the remote server, performing the following: detecting a presence or an absence of a valid hypervisor signature
20 signed with any raw data in the current attestation message; detecting a presence or an absence of an identical precedent for a current timestamp included in the current attestation message from any previous attestation message for a user identity of the current attestation message; if a presence of a valid signature signed with any raw data is detected in the current attestation message, and if an absence
25 of an identical precedent of the current timestamp is detected, ascertaining data

provenance as from authenticated human user; and if an absence of a valid hypervisor signature signed with any raw data is detected in the current attestation message, ascertaining data provenance as from software user.

According to one embodiment of the invention, a client mobile device
5 comprises: a memory storage including a buffer; a display unit; a processor coupled to the memory storage, the buffer and the display unit, and configured to operate a hypervisor having a pre-stored hypervisor signature, the hypervisor is configured, in response to a request to authenticate a user to a remote server via a client application installed in the memory storage, to: clear a buffer and blocking
10 write permission of software on the buffer, intercept an interrupt which is generated after raw data is written into the buffer, and transferring the raw data from the buffer to the hypervisor, unblock write permission of software on the buffer, and sign the raw data with a security information which at least includes a hypervisor signature and a current timestamp, for generating a current attestation message, wherein the
15 processor is further configured to submit the current attestation message to the remote server, wherein if a valid signature signed with any raw data is to be detected present in the current attestation message, and if an identical precedent for the timestamp is to be detected absent from any previous attestation message for a user identity of the current attestation message, data provenance as from
20 authenticated human user is to be ascertained at the remote server, and wherein if a valid hypervisor signature signed with any raw data is to be detected absent in the current attestation message, data provenance as from software user is to be ascertained at the remote server.

According to one embodiment of the invention, a server computer
25 comprises: a memory storage having a plurality of pre-assigned hypervisor

signatures, and a plurality of timestamps and previous attestation messages; a processor which is coupled to the memory and configured to: receive a current attestation message; detect a presence or an absence of a valid hypervisor signature signed with any raw data in the current attestation message; detect a
5 presence or an absence of an identical precedent for a current timestamp included in the current attestation message from any of previous attestation message for a user identity of the current attestation message; if a presence of a valid signature signed with any raw data is detected in the current attestation message, and if an absence of an identical precedent of the current timestamp is detected, ascertain
10 data provenance as from authenticated human user; and if an absence of a valid hypervisor signature signed with any raw data is detected in the current attestation message, ascertain data provenance as from software user.

Brief Description of the Drawings

Embodiments of the invention are disclosed hereinafter with reference to the
15 drawings, in which:

Figure 1 shows a secured communication system according to one embodiment of the invention;

Figure 2 shows a simplified architecture configuration of a client mobile device according to one embodiment of the invention;

20 Figure 3 shows a flow sequence for remote attestation of data provenance according to one embodiment of the invention;

Figure 4A shows a rootkit attack on a transaction in a prior art system; and

Figure 4B shows attestation of data provenance in the example of Figure 4A according to one embodiment of the invention.

Detailed Description

In the following description, numerous specific details are set forth in order
5 to provide a thorough understanding of various illustrative embodiments of the invention. It will be understood, however, to one skilled in the art, that embodiments of the invention may be practiced without some or all of these specific details. In other instances, well known process operations have not been described in detail in order not to unnecessarily obscure pertinent aspects of embodiments being
10 described. In the drawings, like reference numerals refer to same or similar functionalities or features throughout the several views.

Figure 1 shows a secured communication system 10 according to one embodiment of the invention. The system comprises a plurality of client mobile devices 12a, 12b, 12c connected to a remote server computer 14 over a network
15 16, e.g. Internet. Examples of mobile devices include, but are not limited to, smart phones, mobile phones and tablets. The remote server computer 14 may provide services such as, but not limited to, online payment, online banking and e-commerce.

Figure 2 shows a simplified architecture configuration of a client mobile
20 device 12 according to one embodiment of the invention. The mobile device 12 includes, amongst others, a display unit (e.g. touch screen), a memory storage including a buffer, and a processor coupled to the display unit, memory storage and buffer. The mobile device 12 is pre-installed with a bare-metal hypervisor which stores a digital signature key pair which are certified by a trusted authority.

The hypervisor runs directly on the device hardware and underneath the operating system (OS) e.g. Android. In certain embodiments, the hypervisor runs in the ARM CPU's HYP mode with a higher privilege than the OS. Accordingly, the hypervisor is capable of managing hardware and intercepting interrupts, exceptions and traps.

5 The hypervisor is also capable of configuring control bits of page table entries to define memory access rights of the operating system and other software. For example, the hypervisor can block all software access to the touch screen's frame buffer. In the mobile device 12, at least one client application is installed in the memory storage to operate on the OS.

10 Figure 3 shows a flow sequence 300 for attestation of data provenance according to one embodiment of the invention. In this embodiment, it is assumed that a user enters input (authentication) data into a mobile device 12 via a software keyboard. The flow sequence 300 is initiated when a user submits a request via a client application to authenticate the user to a remote server. When the user starts
15 to input data through a peripheral device, e.g. software keyboard, the client application issues a first hypercall to the hypervisor to request attestation (block 302).

In response to the first hypercall, the hypervisor clears a DMA (Direct Memory Access) buffer and blocks write permission of software, including both the
20 client application and OS, on the buffer (block 304). Particularly, the buffer is set read-only by setting attribute bits of corresponding page table entries in Stage-2 page table of the platform. Accordingly, software and the OS cannot write to the DMA buffer whereas mobile device hardware can write to the DMA buffer.

Input or raw data (e.g. (x,y) coordinates of the user's taps on the touch screen of the mobile device) received from the user via the mobile device hardware is written to the buffer and an interrupt is generated (block 306).

5 The hypervisor intercepts the interrupt and transfers the raw data to the hypervisor (block 308). The hypervisor then passes the interrupt to the operating system which then fetches and processes the raw data. The step of intercepting the interrupt and transferring raw data to the hypervisor is repeated while further raw data may be produced.

10 At the end of raw data entry, the client application issues a second hypercall to notify the hypervisor. In response to the second hypercall, the hypervisor ceases intercepting the interrupt and unblocks write permission of software, including both the client application and the OS, on the buffer (block 310).

15 The client application converts the raw data to application data (e.g. (x,y) coordinates to corresponding character or number), submits the application data to a remote server and issues a third hypercall to request the hypervisor's attestation (block 312).

20 In response to the third hypercall, the hypervisor signs the raw data residing in the hypervisor space with security information (block 314). The security information at least includes a hypervisor signature key which was pre-stored in the hypervisor and pre-assigned to a user-specified mobile device, and a current timestamp representing the time of signing the raw data. In certain embodiments, the security information may further include a unique identifier of the mobile device (e.g. IMEI).

The signed raw data is returned to the client application which then submits an attestation message to the remote server for verification (block 316). In this embodiment, the attestation message at least includes the signature, the raw data and the timestamp.

5 At the remote server, the server receives the attestation message and performs verification based on the attestation message (block 318). In this embodiment, the verification is performed in two stages.

The first verification stage (block 320) involves verifying data provenance as from hardware/human user (hereinafter referred to as “human user”) or from
10 software user (e.g. malware), verifying user authenticity, and verifying uniqueness of a timestamp included in the current attestation message for a particular user identity.

Verifying data provenance as from human user or software user involves detecting a presence or absence of any hypervisor signature signed with any raw
15 data.

Verifying user authenticity involves ascertaining validity of the hypervisor signature included in the attestation message (i.e. whether the received hypervisor signature corresponds to a pre-assigned hypervisor signature associated with a user identity of the attestation message). Verification of user authenticity may be
20 performed by a signature verification procedure as known in the art.

Verifying uniqueness of a timestamp in the attestation message involves detecting a presence or an absence of an identical precedent for a current timestamp included in the current attestation message from any previous attestation message for a user identity of the current attestation message. If an

identical precedent timestamp for the same user identity is detected present from any previous attestation message, this implies that a previously-generated hypervisor signature is being re-used in the current attestation message. However, if an identical precedent timestamp for the same user identity is detected absent
5 from previous attestation message(s), this implies the timestamp in the current attestation is unique for the user identity of the current attestation message.

In block 320, if any hypervisor signature signed with any raw data is detected present in the current attestation message, the hypervisor signature is ascertained valid, and an identical precedent timestamp is detected absent in
10 previous attestation message(s) for the user identity associated with the current attestation message, the first verification step ascertains data provenance as from authenticated human user. If the current attestation message does not include any hypervisor signature signed with any raw data, the first verification step ascertains data provenance as from software user (e.g. malware). It is to be appreciated that
15 if a malware attempts to impersonate a human user, the above-described sequence would not receive raw data into the hypervisor (in block 308) since write permission of the client application and OS has been blocked and therefore the step of the hypervisor signing raw data with a security information (in block 314) would not result in the expected signed raw data. Further, it may be determined in
20 that if any hypervisor signature signed with any raw data is detected present in the current attestation message but the hypervisor signature is ascertained invalid, the first verification stage ascertains data provenance as from unauthenticated (or imposter) human user. Yet further, it may be determined that if any hypervisor signature signed with any raw data is detected present in the attestation message,
25 the hypervisor signature is ascertained valid, but an identical precedent timestamp

is ascertained for the user identity associated with the current attestation message, the first verification stage ascertains data provenance as from software user.

The second verification stage (block 322) is performed if the first verification stage is successful, i.e. ascertains data provenance as from human user, hypervisor signature is ascertained valid, and no identical precedent timestamp is detected (i.e. conditions for establishing authenticated human user are satisfied). In the second verification stage, the server converts the raw data (e.g. (x,y) coordinates) which is included in the attestation message to application data (e.g. character or number) in a similar manner as the client application. It is to be appreciated that the mobile device and server would have been provided a predetermined way of interpreting raw data inputted to the mobile device, for example, both the mobile device and server have been provided with a common software keyboard having fixed layout, screen location and size. If the converted raw data, which is ascertained by the server, corresponds to the application data provided by the client application in block 312, the second verification stage is successful, i.e. corroborate or further confirm data provenance is from authenticated human user. If the converted input data which is ascertained by the server does not match the application data provided in the attestation message by the client application, the second verification stage is unsuccessful, i.e. data provenance integrity is compromised—raw data may originate from malware.

If both the first and second verification stages are successful, the attestation process is successful and accordingly the raw data and application data are accepted by the server which then proceeds further to handle or process the transaction. If either the first or the second verification stage is unsuccessful, the

attestation fails and a security issue or breach is identified. In this case, the server would not accept the raw data nor proceed with the transaction.

The flow sequence of Figure 3 may be modified in other embodiments of the invention. Possible modifications are described below and may be employed
5 individually or in combination:

In certain embodiments, identity of the mobile device is further verified in block 318. To this purpose, security information (in block 314) signed with the raw data further includes a unique mobile device identifier, e.g. International Mobile Equipment Identity (IMEI). Verification at the remote server (in block 318) may
10 further include verification of the mobile device identity, by ascertaining whether the unique mobile device identifier included in the attestation message is associated with a user identity of the attestation message. If an association is present, the present mobile device is authenticated and data provenance is ascertained as from authenticated human user if other above-described verification criteria are satisfied.
15 However, if an association is not present, verification fails and the present mobile device is ascertained as an imposter mobile device.

In certain embodiments, raw data is inherently useful and does not require conversion to application data. Consequently, in block 318, the verification at the server requires only the first verification stage. Examples of such raw data include,
20 but are not limited to, location data, biometric data, fingerprint data, camera data and motion sensor data.

Embodiments of the invention may be applied to various situations including but not limited to the following examples.

Example I: User Authentication

This example involves running a client application to authenticate a user to a remote server by supplying the user password. A malware residing in the mobile device with root privilege may capture the user password in a few ways, such as,
5 (1) impersonating the user by logging to the server automatically, (2) leaking the password to a remote human adversary who impersonates the victim manually. In this example, the client application and server share a common software keyboard with identical layout, screen position and size; therefore the software keyboard does not need to be protected.

10 In the first attack, a malware generates data and attempts to write this data to a DMA buffer. Since the DMA buffer is write-protected, the malware cannot write to the DMA buffer and therefore the hypervisor cannot sign data generated by the malware. When an attestation message is submitted to the server for verification, the message would not contain the hypervisor's attestation and would therefore fail
15 the verification. Previous attestation cannot be re-used as the hypervisor's attestation includes a timestamp.

In the second attack, the human imposter impersonates a victim's identity using the any mobile device other than the victim's. Although the human imposter is able to obtain a hypervisor's attestation, the signature is bound to an identity
20 other than the victim's as the imposter's mobile device does not own the private signature key assigned to the victim's hypervisor. Even if the server has prior knowledge of the public key certificate of the victim's hypervisor, the victim's hypervisor signature key is securely protected and stored in the hypervisor space of the victim's mobile device such that no malware can access it.

Example II: Biometric-Based Authentication

Biometric features (e.g. fingerprints) have been widely used in online remote authentication systems to enhance the security. One of the key challenges of biometric-based authentication is to detect the freshness of the biometric data, in order to tackle malware replay attacks where previously-captured biometric data are re-used.

If a fingerprint reader collects a user's fingerprint and places this data in the I/O buffer via DMA, the hypervisor write-protect the I/O buffer to prevent a malware from writing data thereto. The hypervisor intercepts the DMA complete interrupt and signs the data residing in the buffer. The signature is an attestation that the data are due to human user actions, i.e. a finger is placed on the fingerprint reader.

Example III: Sensitivity of Numbers in Transactions

This example involves a Payment Gateway (PG) which is an online banking server and a user running a Payment App (PA) to request a bank transfer. If the user intends to transfer \$100 to a particular account, the user enters numeric inputs '100' on a software keyboard displayed on the touchscreen of the user's mobile device.

In a prior art system as shown in Figure 4A, a rootkit in a mobile device can modify the user's input data '100' to '100,000' before submitting the modified data to the Payment Gateway. The rootkit may modify the user's input in a few ways, such as, (1) tamper with the data path between the device hardware and the application or (2) attack the user interface.

Applying the invention to this example as shown in Figure 4B, it is assumed the Payment App and Payment Gateway share a standard number pad for inputting numerical values.

In the first attack, the rootkit intervenes after a DMA operation. Any data
5 modification would not match the original input value attested by the hypervisor,
and would therefore be detected by the Payment Gateway upon verification of the
attestation message. More particularly, in the attestation message submitted to the
Payment Gateway, the (x,y) coordinates of the user input data signed by the
hypervisor would not match the application data and/or (x,y) coordinates which
10 were modified by the rootkit.

In the second attack, the malware may manipulate the user interface to
deceive the user into inputting more digits than the user had intended to. In this
circumstance, the above-described embodiments of the invention may be modified
to defeat this threat of fraudulent interface as described in the following.

15 Particularly, the hypervisor converts the raw data entered by the user into
numbers by using the standard number pad layout, and securely writes the
converted raw data into the touchscreen's frame buffer. The frame buffer is locked
by the hypervisor so that neither the operating system nor any application has
access to it. By displaying the converted raw data (e.g. inputted number) on the
20 screen, the hypervisor notifies the human user of the inputted number for user
verification. Depending on whether the displayed number or information is
anomalous, the human user may choose to terminate or proceed with the
transaction. Accordingly, malware's modification of user inputs would be detected
and arrested prior to proceeding with a transaction.

As will be appreciated from the above, embodiments of the invention provide improved mobile security. Particularly, the invention provides a solution against rootkit attacks, by verifying whether data is inputted by a human user or a software user since software user (e.g. malware) cannot produce raw data entry through
5 device hardware.

Also, the hypervisor attestation provides a second factor for authentication by ensuring that a compromised user credential (e.g. a user password or a fingerprint template) alone does not lead to illegal access to the user's (victim's) account. Further, the signature from the hypervisor can serve as a non-repudiating
10 evidence such that the mobile device owner cannot deny the transaction.

Other embodiments will be apparent to those skilled in the art from consideration of the specification and practice of the invention. Furthermore, certain terminology has been used for the purposes of descriptive clarity, and not to
15 limit the disclosed embodiments of the invention. The embodiments and features described above should be considered exemplary.

Claims

1. A method implementable at a mobile device for attestation of data provenance, the method comprising:

5 in response to a request to authenticate a user to a remote server via a client application which resides in the mobile device, performing the following by a hypervisor:

clearing a buffer and blocking write permission of software on the buffer,

10 intercepting an interrupt which is generated after raw data is written into the buffer, and transferring the raw data from the buffer to the hypervisor,

unblocking write permission of software on the buffer,

15 signing the raw data with a security information which at least includes a hypervisor signature and a current timestamp, for generating a current attestation message; and

submitting the current attestation message to the remote server,

wherein if a valid signature signed with any raw data is to be detected present in the current attestation message, and if an identical precedent for the current timestamp is to be detected absent from any previous attestation message for a
20 user identity of the current attestation message, data provenance as from authenticated human user is to be ascertained at the remote server, and

wherein if a valid hypervisor signature signed with any raw data is to be detected absent in the current attestation message, data provenance as from software user is to be ascertained at the remote server.

- 5 2. The method of claim 1, wherein the security information further includes a unique identifier of the mobile device, and

wherein if a valid signature signed with any raw data is to be detected present in the current attestation message, if an identical precedent for the current timestamp is to be detected absent from any previous attestation message for a user identity
10 of the current attestation message, and if an association of the unique mobile device identifier with the user identity of the current attestation message is detected present, data provenance as from authenticated human user is to be ascertained at the remote server.

- 15 3. The method of any of claims 1 to 2, further comprising:

converting the raw data to an application data and submitting the application data to the remote server,

wherein if the application data is to be ascertained corresponding to a converted form of the raw data included in the current attestation message, the ascertained
20 data provenance as from authenticated human user is to be corroborated.

4. The method of any of claims 1 to 3, further comprising:

prior to unblocking write permission, converting the raw data, and

presenting the converted data on a display unit of the mobile device for user verification.

5. A method implementable at a server for attestation of data provenance, the
5 method comprising:

receiving a current attestation message;

detecting a presence or an absence of a valid hypervisor signature signed
with any raw data in the current attestation message;

detecting a presence or an absence of an identical precedent for a current
10 timestamp included in the current attestation message from any previous
attestation message for a user identity of the current attestation message;

if a presence of a valid signature signed with any raw data is detected in the
current attestation message, and if an absence of an identical precedent of the
current timestamp is detected, ascertaining data provenance as from authenticated
15 human user; and

if an absence of a valid hypervisor signature signed with any raw data is
detected in the current attestation message, ascertaining data provenance as from
software user.

- 20 6. The method of claim 5, further comprising:

detecting a presence or an absence of an association of a unique mobile
device identifier included in the current attestation message with the user identity of
the current attestation message; and

if an association of a unique mobile device identifier included in the current attestation message with the user identity is additionally detected present, ascertaining data provenance as from authenticated human user.

5 7. The method of any of claims 6 to 7, further comprising:

receiving an application data;

after ascertaining data provenance as from authenticated human user, converting raw data included in the current attestation message and verifying the converted raw data against the application data, and

10 if the converted raw data corresponds to the application data, corroborating data provenance as from authenticated human user.

8. A method for attestation of data provenance, the method comprising:

in response to a request to authenticate a user to a remote server via a
15 client application which resides in a mobile device, performing the following by a hypervisor:

clearing a buffer and blocking write permission of software on the
buffer,

intercepting an interrupt which is generated after raw data is written
20 into the buffer, and transferring the raw data from the buffer to the hypervisor,

unblocking write permission of software on the buffer, and

signing the raw data with a security information which at least includes a hypervisor signature and a current timestamp for generating a current attestation message;

submitting the attestation message to the remote server; and

5 at the remote server, performing the following:

detecting a presence or an absence of a valid hypervisor signature signed with any raw data in the current attestation message;

10 detecting a presence or an absence of an identical precedent for a current timestamp included in the current attestation message from any previous attestation message for a user identity of the current attestation message;

15 if a presence of a valid signature signed with any raw data is detected in the current attestation message, and if an absence of an identical precedent of the current timestamp is detected, ascertaining data provenance as from authenticated human user; and

if an absence of a valid hypervisor signature signed with any raw data is detected in the current attestation message, ascertaining data provenance as from software user.

20 9. The method of claim 1, wherein the security information further includes a unique identifier of the mobile device, wherein the method further comprising:

at the remote server:

detecting a presence or an absence of an association of a unique mobile device identifier included in the current attestation message with the user identity of the current attestation message;

if an association of a unique mobile device identifier included in the current attestation message with the user identity is additionally detected present, ascertaining data provenance as from authenticated human user.

10. The method of any of claims 8 to 9, further comprising:

submitting an application data from the client application to the remote server;

wherein at the remote server, after ascertaining data provenance as from authenticated human user:

converting the raw data included in the current attestation message and verifying the converted raw data against the application data, and

if the converted raw data corresponds to the application data, corroborating data provenance as from authenticated human user.

11. The method of any of claims 8 to 10, wherein performing the following by a hypervisor further includes:

prior to unblocking write permission, converting the raw data, and

presenting the converted data on a display unit of the mobile device for user verification.

12. A client mobile device comprising:

memory storage including a buffer;

a display unit;

a processor coupled to the memory storage, the buffer and the display unit,

5 and configured to operate a hypervisor having a pre-stored hypervisor signature,
the hypervisor is configured, in response to a request to authenticate a user to a
remote server via a client application installed in the memory storage, to:

clear a buffer and blocking write permission of software on the buffer,

intercept an interrupt which is generated after raw data is written into

10 the buffer, and transferring the raw data from the buffer to the hypervisor,

unblock write permission of software on the buffer, and

sign the raw data with a security information which at least includes a
hypervisor signature and a current timestamp, for generating a current
attestation message,

15 wherein the processor is further configured to submit the current attestation
message to the remote server,

wherein if a valid signature signed with any raw data is to be detected present in
the current attestation message, and if an identical precedent for the timestamp is
to be detected absent from any previous attestation message for a user identity of
20 the current attestation message, data provenance as from authenticated human
user is to be ascertained at the remote server, and

wherein if a valid hypervisor signature signed with any raw data is to be detected
absent in the current attestation message, data provenance as from software user
is to be ascertained at the remote server.

13. The client mobile device of claim 12, wherein the hypervisor is configured to sign the raw data with the security information which further includes a unique identifier of the mobile device, and

wherein if a valid signature signed with any raw data is to be detected present in
5 the current attestation message, if an identical precedent for the timestamp is to be detected absent from any previous attestation message for a user identity of the current attestation message, and if an association of the unique mobile device identifier with the user identity of the current attestation message is detected present, data provenance as from authenticated human user is to be ascertained
10 at the remote server.

14. The client mobile device of any one of claims 12 to 13, wherein the processor is further configured to convert the raw data to an application data and submit the application data to the remote server,

15 wherein if the application data is to be ascertained corresponding to a converted form of the raw data included in the current attestation message, the ascertained data provenance as from authenticated human user is to be corroborated.

15. The client mobile device of any of claims 12 to 14, wherein the processor is
20 further configured to convert the raw data and present the converted data on a display unit of the mobile device for user verification.

16. A server computer comprising:

a memory storage having a plurality of pre-assigned hypervisor signatures,
and a plurality of timestamps and previous attestation messages;

a processor which is coupled to the memory and configured to:

5 receive a current attestation message;

 detect a presence or an absence of a valid hypervisor signature
signed with any raw data in the current attestation message;

 detect a presence or an absence of an identical precedent for a
current timestamp included in the current attestation message from any of
10 previous attestation message for a user identity of the current attestation
message;

 if a presence of a valid signature signed with any raw data is detected
in the current attestation message, and if an absence of an identical
precedent of the current timestamp is detected, ascertain data provenance
15 as from authenticated human user; and

 if an absence of a valid hypervisor signature signed with any raw data
is detected in the current attestation message, ascertain data provenance as
from software user.

20 17. The server computer of claim 16, wherein the processor is further configured
to:

detect a presence or an absence of an association of a unique mobile device identifier included in the current attestation message with the user identity of the current attestation message; and

if an association of a unique mobile device identifier included in the current
5 attestation message with the user identity is additionally detected present, ascertain data provenance as from authenticated human user.

18. The server computer of any one of claims 16 and 17, wherein the processor is further configured to:

10 receive an application data;

after ascertaining data provenance as from authenticated human user, convert raw data included in the current attestation message and verify the converted raw data against the application data, and

if the converted raw data corresponds to the application data, corroborate data
15 provenance as from authenticated human user.