US 20220021693A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2022/0021693 A1

Summers et al. (43) Pub. Date: Jan. 20, 2022

(54) **TRUSTED TRAVEL DEVICES EQUIPPED WITH ON-THE-FLY MONITORING**

(71) Applicant: **Bank of America Corporation**, Charlotte, NC (US)

(72) Inventors: **Harvey Summers**, Richmond, VA (US); **Vijaya L. Vemireddy**, Plano, TX (US); **Brandon Sloane**, Charlotte, NC (US); **Eileen D. Bridges**, Fort Mill, SC (US)

(21) Appl. No.: **16/928,797**

(22) Filed: **Jul. 14, 2020**

Publication Classification

(51) **Int. Cl.**

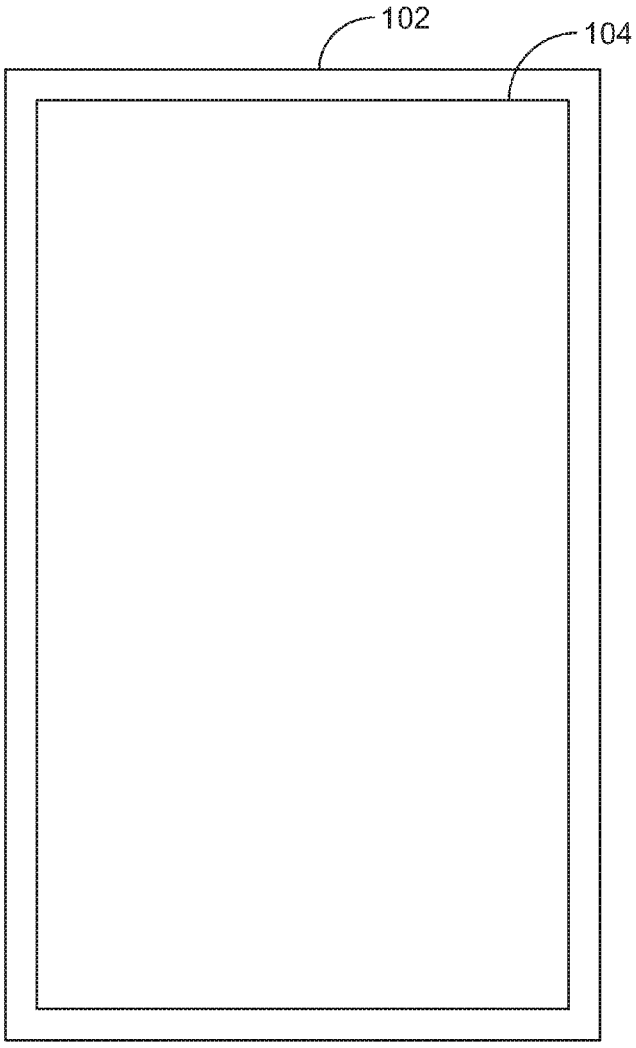
H04L 29/06	(2006.01)
G06F 1/14	(2006.01)
G06F 8/61	(2006.01)
H04L 12/26	(2006.01)

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

CPC ***H04L 63/1425*** (2013.01); ***G06F 1/14*** (2013.01); *G06Q 10/1093* (2013.01); ***H04L 63/1475*** (2013.01); ***H04L 43/08*** (2013.01); ***G06F 8/61*** (2013.01)

(57) **ABSTRACT**

A method for enhancing travel security features associated with a mobile device is provided. The method may include operating a time clock on the mobile device to determine a start device confiscation time in the memory and to determine an end device confiscation time in the memory. The method may also include monitoring the operation of the mobile device between the start device confiscation time and the end device confiscation time to determine the existence of an anomalous device condition. The monitoring may include using a network traffic monitor device, a bandwidth usage monitor device, a battery performance monitor device, a website presentation monitor device, and/or central processing usage monitor device. The monitoring may record a device activity between the start time and the end time and flag the anomalous device condition that occurred between the start time and the end time.



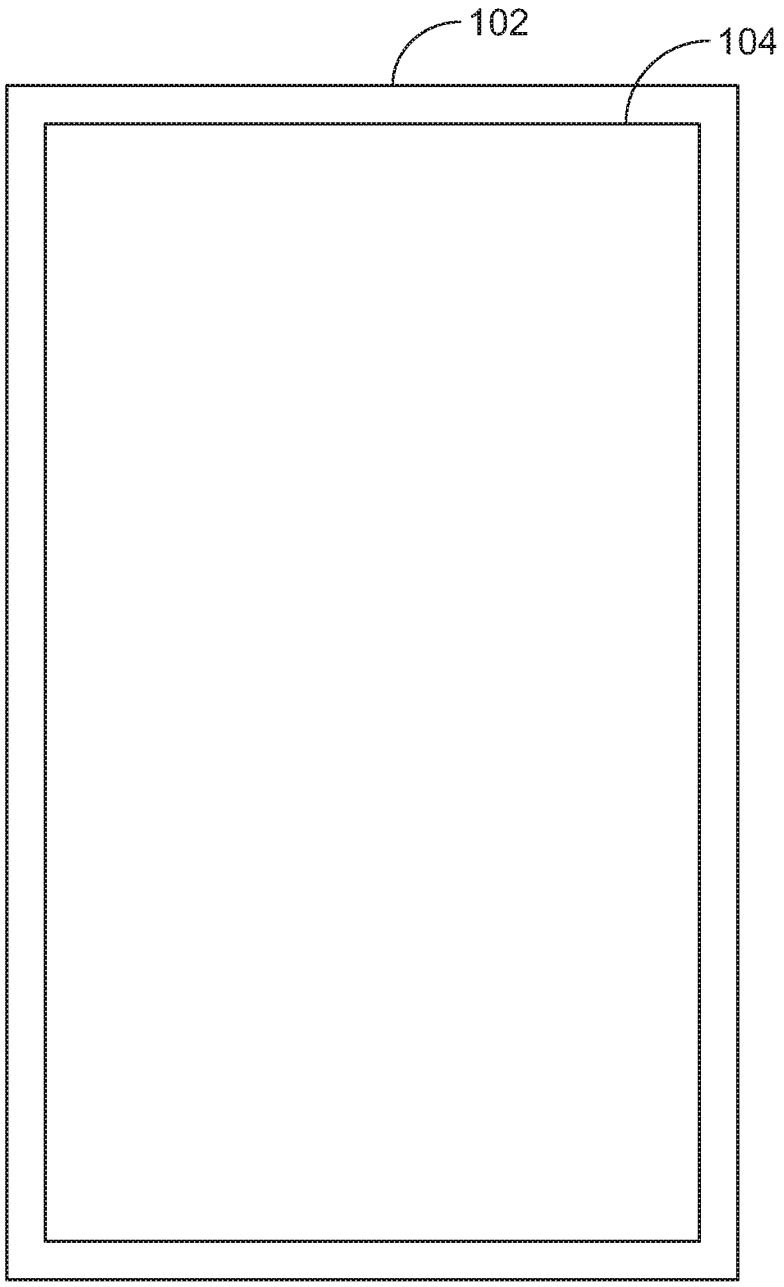


FIG. 1

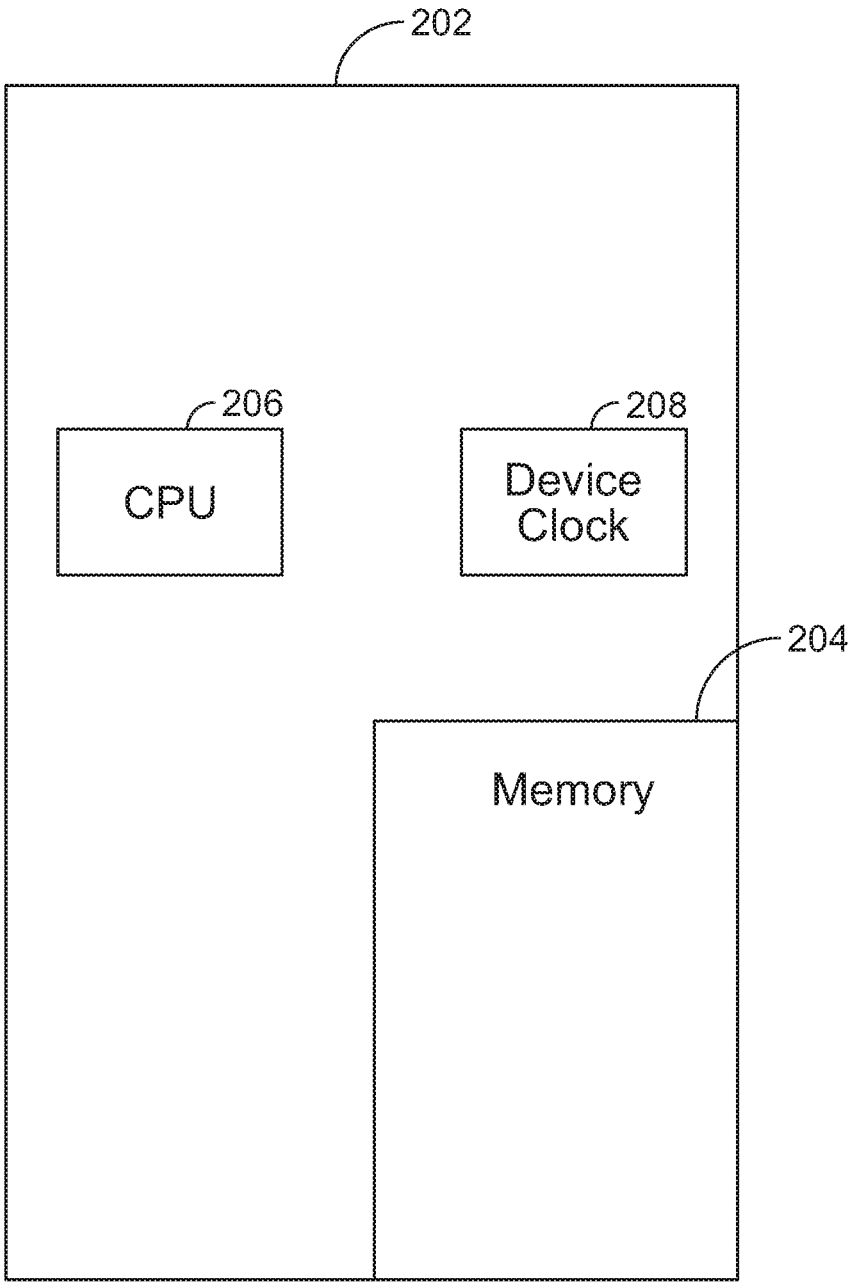


FIG. 2

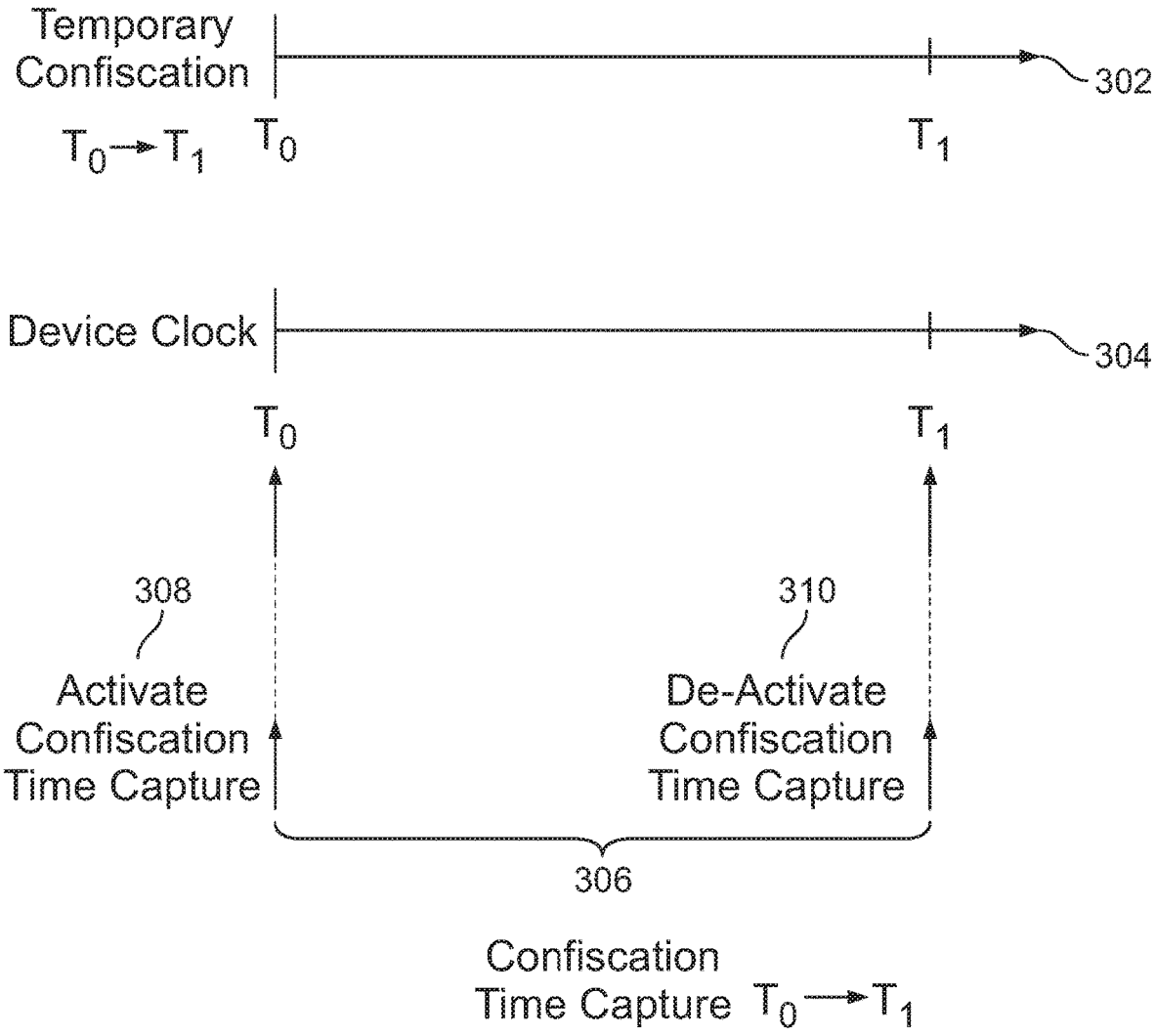

Temporary Confiscation
$T_0 \rightarrow T_1$
T_0
T_1
302
Device Clock
304
T_0
T_1
308
Activate Confiscation Time Capture
310
De-Activate Confiscation Time Capture
306
Confiscation Time Capture $T_0 \rightarrow T_1$

FIG. 3

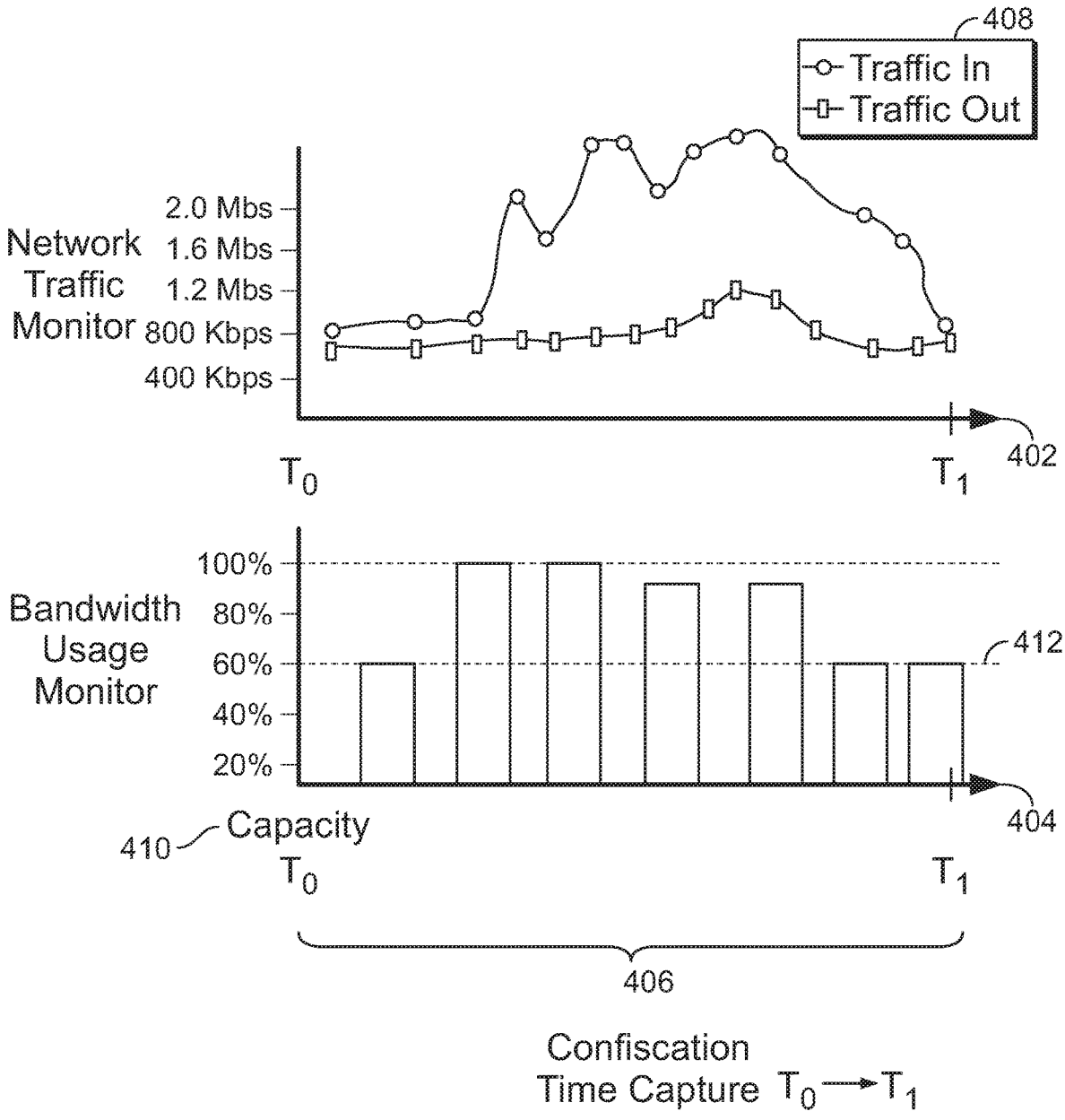

408
Traffic In
Traffic Out
Network Traffic Monitor
2.0 Mbs
1.6 Mbs
1.2 Mbs
800 Kbps
400 Kbps
402
T_0
T_1
Bandwidth Usage Monitor
100%
80%
60%
40%
20%
412
404
410
Capacity
T_0
T_1
406
Confiscation Time Capture $T_0 \rightarrow T_1$

FIG. 4

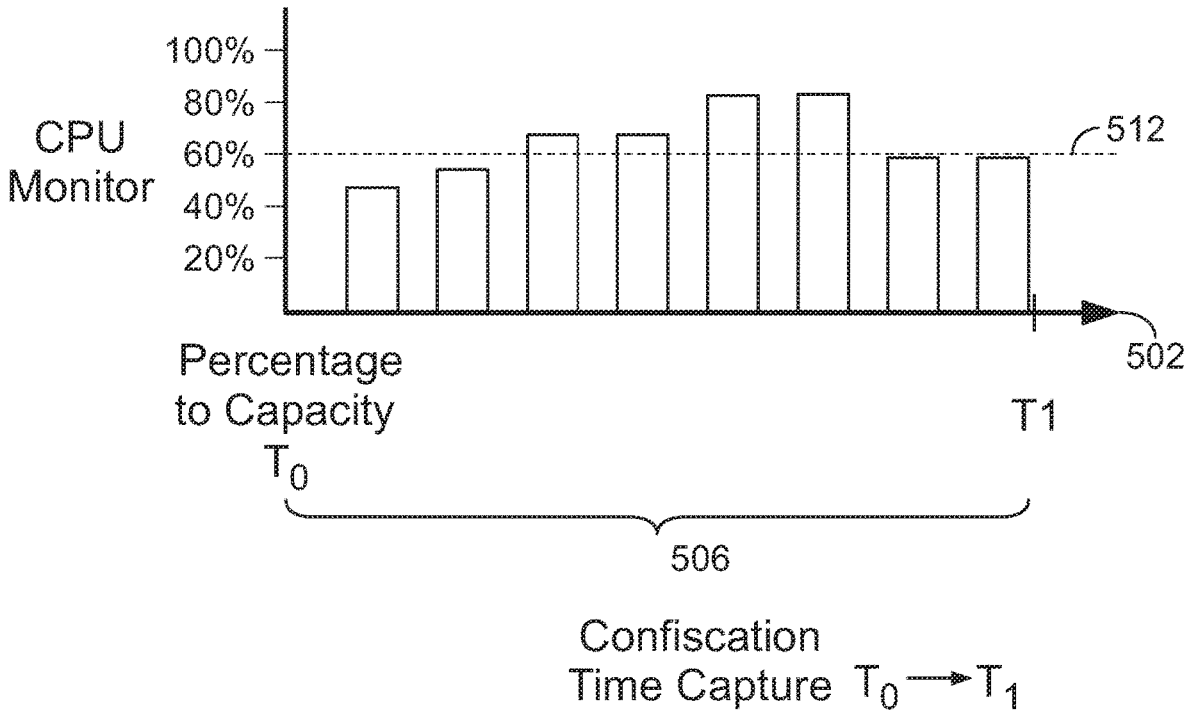

CPU
Monitor
100%
80%
60%
40%
20%
512
502
Percentage
to Capacity
T0
T1
506
Confiscation
Time Capture T0 → T1

FIG. 5

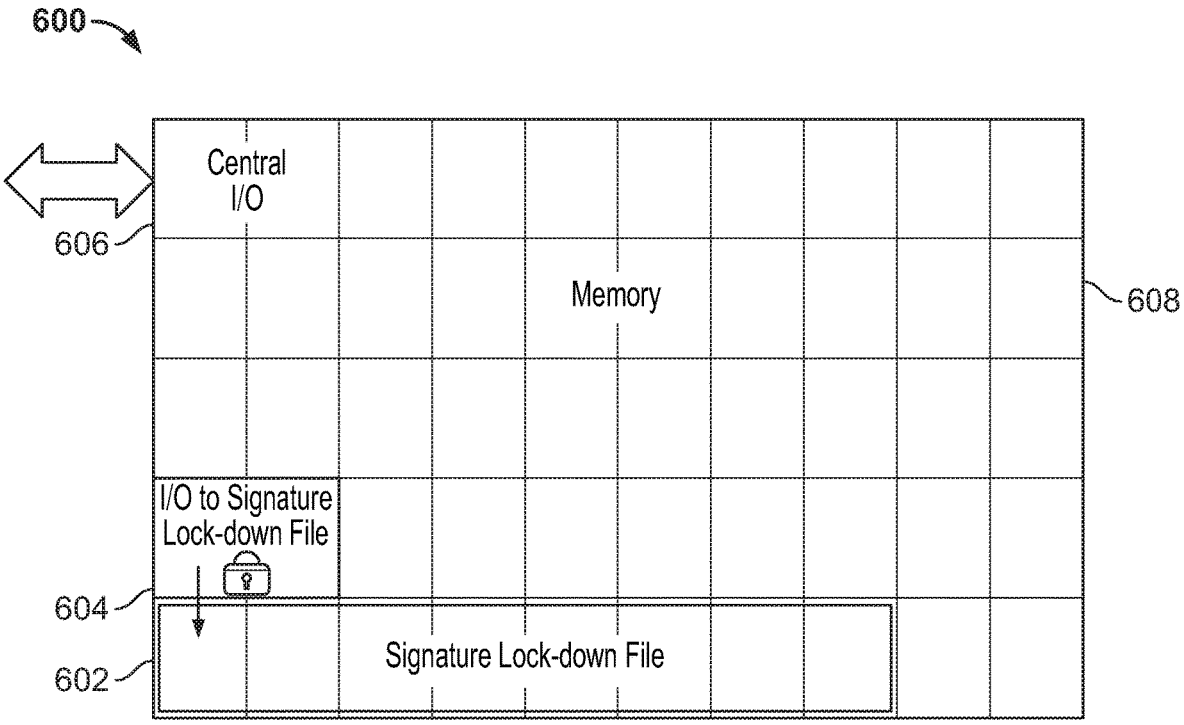

600
Central I/O
606
Memory
608
I/O to Signature Lock-down File
604
Signature Lock-down File
602

FIG. 6

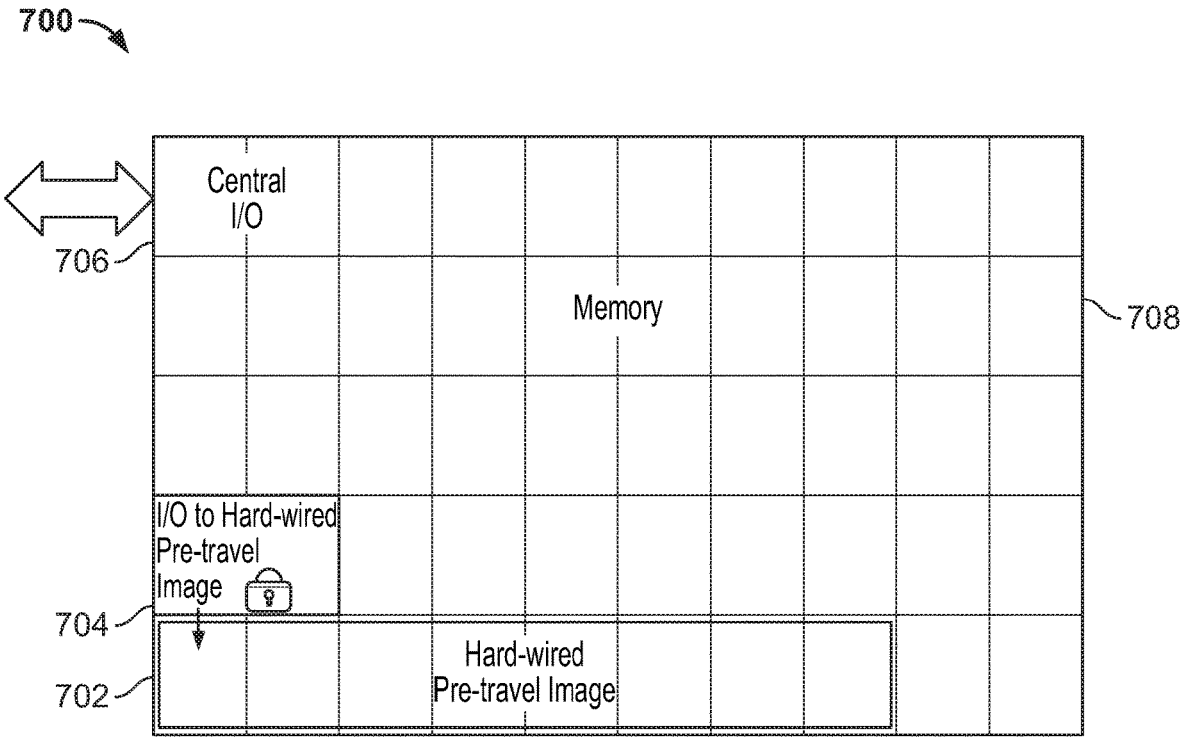

700
Central I/O
706
Memory
708
I/O to Hard-wired Pre-travel Image
704
Hard-wired Pre-travel Image
702

FIG. 7

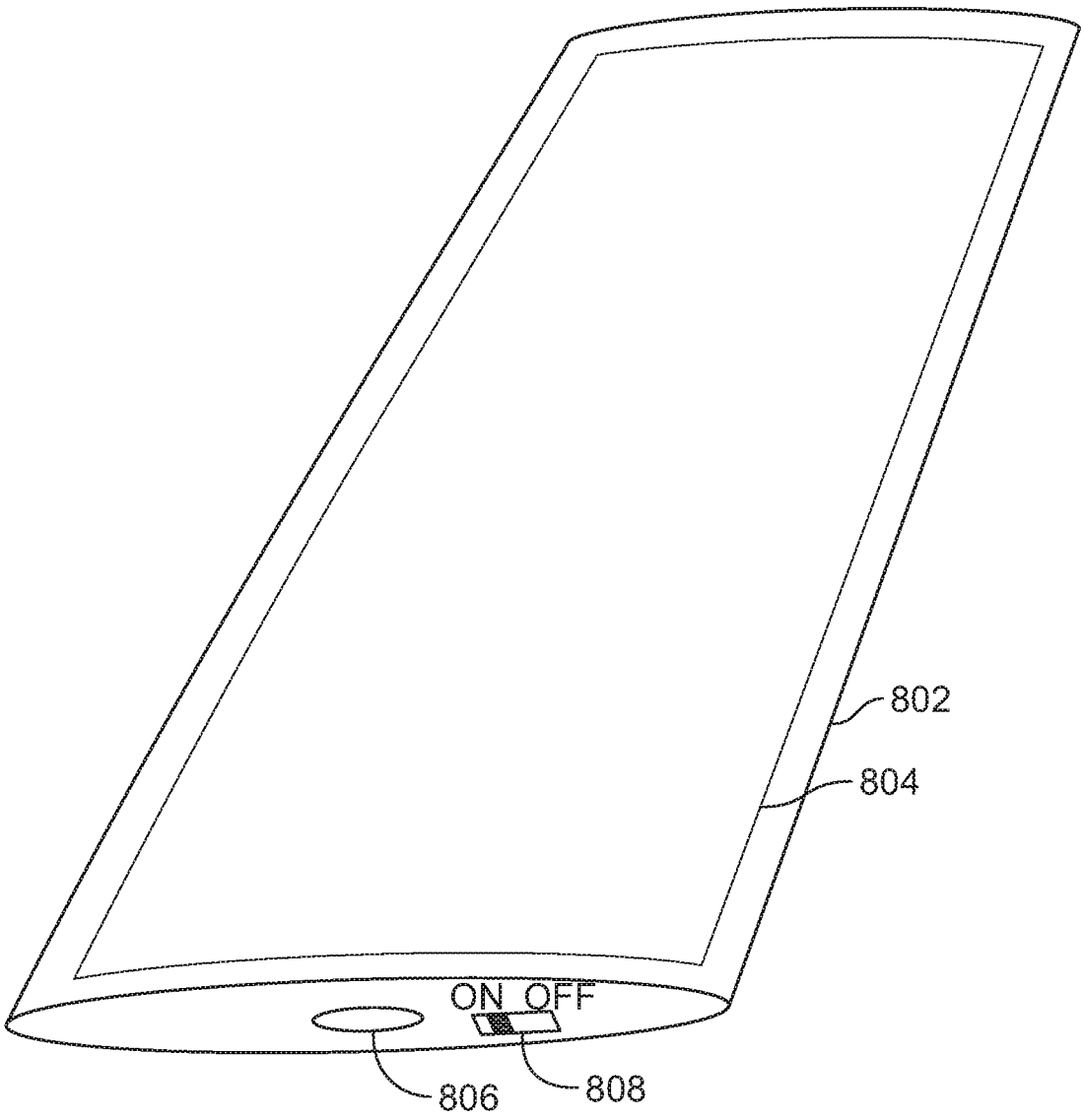


FIG. 8

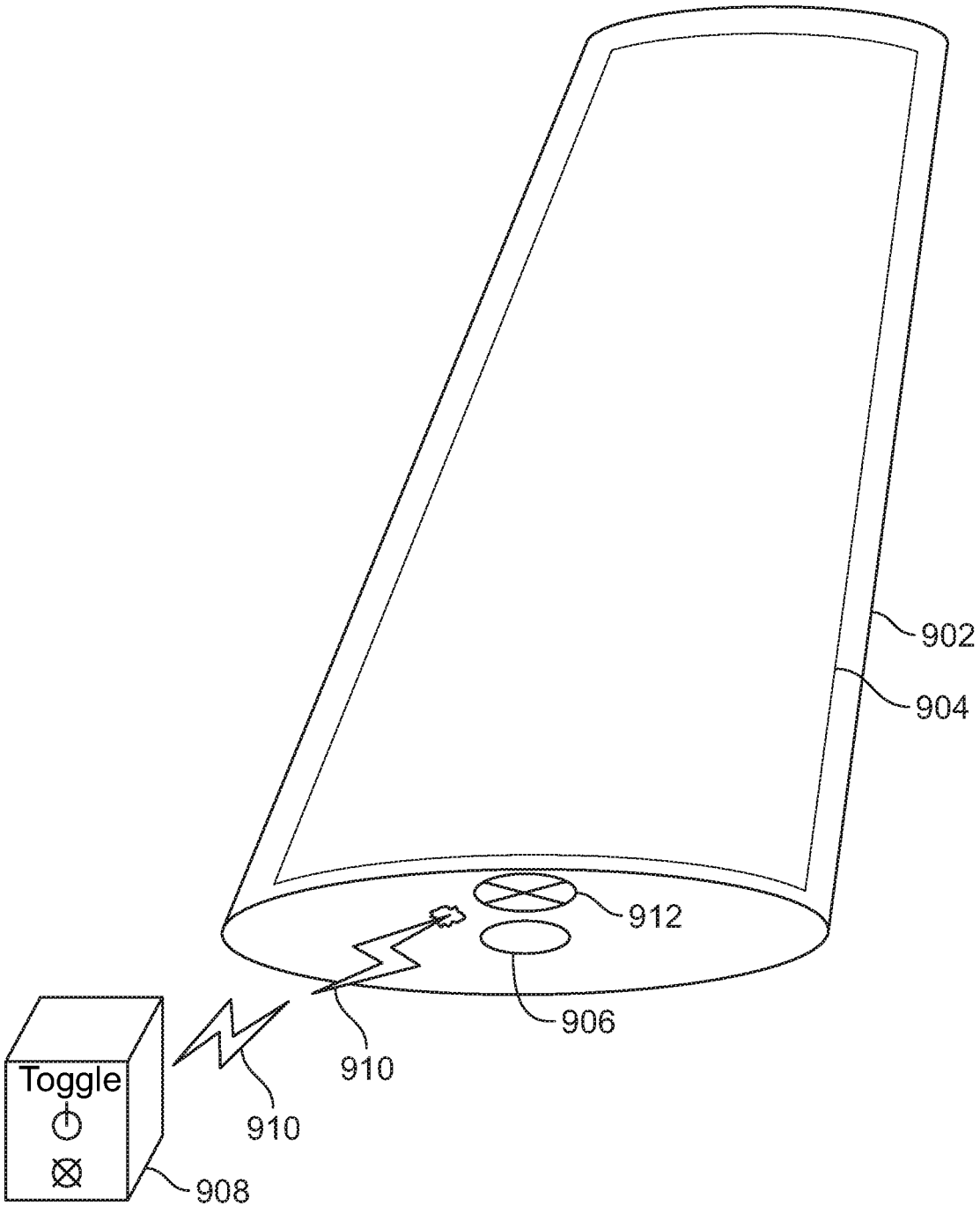


FIG. 9

TRUSTED TRAVEL DEVICES EQUIPPED WITH ON-THE-FLY MONITORING

FIELD OF TECHNOLOGY

[0001] This disclosure relates to trusted travel devices.

BACKGROUND

[0002] When a person is travelling, one or more of his devices may be removed from his possession for investigation. Such removal may include inspection. Such removal may include tampering. Such tampering may include installing wire-tapping applications on the mobile device. Such tampering may involve installing other listening or logging devices on the mobile device.

[0003] Various conventional approaches exist to responding to such confiscation, tampering and installation of such listening devices. These approaches include browser containerization, virtual sandbox, etc., in order to allow for continued secure web interaction during travel. As technology develops further, it is important to continue to improve mobile devices, and methods for using the mobile devices, that are secure.

[0004] Further, it would be desirable to provide systems and methods that mitigate the possibility of breach of mobile device security.

[0005] It would be further desirable to provide systems and methods that identify the occurrence of such tampering and/or other breach.

[0006] Assuming breach, it would be desirable to provide systems and methods that can remediate a post-breach condition.

SUMMARY OF THE DISCLOSURE

[0007] It is an object of this disclosure to provide systems and methods that mitigate the possibility of such breach.

[0008] It is an object of this disclosure to provide systems and methods that identify the occurrence of such tampering and/or other breach.

[0009] It is an object of this disclosure to provide systems and methods that can remediate a post-breach condition.

[0010] A mobile device according to certain embodiments may include enhanced travel security features. The mobile device may include a memory. The mobile device may include a settable time clock. For the purposes of this application a settable time clock (alternatively referred to herein as a "device clock" or "time clock") refers to a timing device that may be first initiated and then stopped. The time between the initiation and the stopping may be considered a confiscation time.

[0011] The time clock may operate or be configured to store a start device confiscation time in the memory and to store an end device confiscation time in the memory.

[0012] The mobile device may also include at least one monitor device selected from the group consisting of a network traffic monitor device, a bandwidth usage monitor device and central processing usage monitor device. Other monitoring devices are also possible. Such other monitoring devices may include a battery performance monitor device and/or a website presentation monitor device. One or more of the monitoring devices may be used to determine whether an anomalous event occurred during the time that the mobile device had been confiscated.

[0013] At least one of the monitoring devices listed above may record activity between the start device confiscation time and the end device confiscation time in the memory. At least one of the monitoring devices listed above may flag an anomalous device condition that occurred between the start device confiscation time and the end device confiscation time. The flagging of the anomalous device condition may be based at least in part on an anomalous condition detected by one or more of the monitoring devices.

[0014] In some embodiments, the mobile device may allow for inspection showing user-configured information. This user-configured information may or may not reflect the true state of the mobile device. This information should preferably be provided from a functionally separate container—i.e., a container that exists and functions preferably separate and apart from the core container of the mobile device. Such a mode of self-configurable display preferably provides an appearance of having complied without disclosing secure information. In this mode, secured information is preferably not accessible to a third party.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] The objects and advantages of the invention will be apparent upon consideration of the following detailed description, taken in conjunction with the accompanying drawings, in which like reference characters refer to like parts throughout, and in which:

[0016] FIG. **1** is a schematic diagram of a mobile device in accordance with the principles of the disclosure;

[0017] FIG. **2** is another schematic diagram of a mobile device in accordance with the principles of the disclosure;

[0018] FIG. **3** is a timing diagram of mobile device clock in accordance with the principles of the disclosure;

[0019] FIG. **4** are timing diagrams of an exemplary network traffic monitor and an exemplary bandwidth usage monitor in accordance with the principles of the disclosure;

[0020] FIG. **5** is a timing diagram of a central processing unit (CPU) usage monitor in accordance with the principles of the disclosure;

[0021] FIG. **6** is a schematic diagram of memory for use in systems and/or methods in accordance with the principles of the disclosure;

[0022] FIG. **7** is another schematic diagram of memory for use in systems and/or methods in accordance with the principles of the disclosure;

[0023] FIG. **8** is a mobile device having a port, and an actuation device for locking the port, in accordance with the principles of the disclosure; and

[0024] FIG. **9** is a mobile device having a port, and a wirelessly-triggerable device for locking the port, in accordance with the principles of the disclosure.

DETAILED DESCRIPTION

[0025] Breach protection according to the embodiments may include the ability to lock down one or more ports during confiscation. Such lock-down may preferably be implemented, in certain embodiments, by toggling a lock-down switch. Such port lock-down can protect a prospective tamperer from having any access to the port(s) that would allow tampering.

[0026] Such toggling can be implemented using a hard-wired switch that presents on the exterior of the mobile device. Such a hard-wired switch may mechanically discon-

nect the internal components of the device from the port(s) that may be used for tampering.

[0027] Such toggling can be implemented using a wireless capable device. The wireless capable device may be configured to send a wireless signal to the mobile device. The wireless signal may cause an internal disconnection, such as a software disconnection or hardware disconnection, of the port(s)—thereby blocking access of a prospective tamperer to the internal workings of the mobile device.

[0028] In certain embodiments of the disclosure, an audio and/or visual alarm can indicate the past occurrence of a breach using a strobe on device—or at remote location. Such a breach may include unauthorized electronic communications with the mobile device. Such a breach may include tampering with the electronic components of the mobile device. Such a breach may include implanting a wire-tapping device, a text-tapping device or any other tampering device within the mobile device hardware and/or software.

[0029] In certain embodiments, multi-factor authentication, such a password, a One-Time-Password (OTP), a biometric characteristic, passphrase or other authentication may be required to access the device during travel.

[0030] Other systems and methods for preventing breach may include monitoring the device during the period of confiscation. Such monitoring may include the state of the machine, or some aspect of the machine. Such monitoring may include monitoring and recording performance of certain aspects of the machine during confiscation. Part of the monitoring may include using the phone clock for capturing the window of time of confiscation. Thereafter, the device may be configured to review performance history of a CPU usage monitor, a bandwidth monitor, a network traffic monitor, a website presentation monitor or other relevant monitor to identify device tampering during confiscation.

[0031] In some embodiments, device tampering may be linked to the detection of anomalous behavior derived from the monitoring of one of the listed monitors.

[0032] When breach occurs, some embodiments of the disclosure may involve a hard-wired mechanism that mitigates the effects of the breach. The hard-wired mechanism may reside in the device. The hard-wired mechanism may provide the ability to re-image the device post-breach.

[0033] The re-image is preferably hard-wired to a pre-travel image. The re-image may be pre-loaded in a predetermined, secure, location in the memory. The re-image may include a signature lockdown file. Re-imaging the device to a pre-travel state may preferably eliminate the effects of any tampering.

[0034] In some embodiments of the invention, integrity verification information may also be set up in the predetermined, secure, location in the file. As such, the location in the memory may contain hardware and/or software that preferably cannot be overwritten which contains biometric information, calendar and scheduling information, online-offline timing information and/or any other integrity verification information or other relevant information.

[0035] In some embodiments—the software associated with integrity information may be secured by encryption, hashing algorithms, distributed ledgers such as blockchains or any other suitable security measures. In certain embodiments, such a blockchain may be protected by limiting write access to one or more secure locations on the chain, while allowing read access from numerous locations on the chain.

[0036] Hardware protection for such overwriting may include placing epoxy on the write-access portions of the solder traces and/or the chips themselves that include the secure information. As such, gaining write access to such mechanically protected areas would require a removal of the epoxy, or other protective fixate. This removal would cause destruction of the system prior to allowing the system to be compromised by tamperer.

[0037] In certain embodiments, the device may capture the state of the machine and check the state of the machine prior to and after device inspection. This may be considered mobile threat defense technology. Such technology may include the capability to detect and inform when a security breach has occurred during confiscation. This information may be derived from the delta observed between the pre- and post-confiscation machine.

[0038] Certain embodiments of the disclosure may also include location-based services to help provide additional information, reminders or social distancing, etc. These embodiments may also include sending pro-active notifications to travelers.

[0039] A system for increasing security of mobile devices is provided. The system and/or the mobile device may include enhanced travel security features. The mobile device may include a memory and a settable time clock. The settable time clock may operate to store a start device confiscation time in the memory and to store an end device confiscation time in the memory. At least one monitor device selected from the group consisting of a network traffic monitor device, a bandwidth usage monitor device and a central processing usage monitor device may be used to record the activity between the start device confiscation time and the end device confiscation time in the memory. The monitor device may flag an anomalous device condition that occurred between the start device confiscation time and the end device confiscation time.

[0040] In some embodiments, the start device confiscation time and the end device confiscation time is determined by user command. That is to say—the user may actuate or otherwise initiate the operation of the clock in order to start the operation of the clock at the beginning of the confiscation time. The user may also, under certain conditions or in certain embodiments, actuate or otherwise terminate the operation of the clock in order to record the end point the confiscation time. The clock initiate command may also initiate operation of one or more device monitors of the types of device monitors set forth herein.

[0041] In some embodiments, the start device confiscation time may be fixed and recorded when the mobile device passes a threshold distance from the mobile device user. In some embodiments, the end device confiscation time may be fixed and recorded when the mobile device returns within the threshold distance of the user.

[0042] In certain embodiments, whether the mobile device passes the threshold distance may be determined, at least in part, by calculating a distance between the mobile device and a second device, preferably mobile, located on the user's person.

[0043] In other embodiments, whether the mobile device passes the threshold distance can be determined, at least in part, by calculating a travel time following removal of the mobile device from the person of the user until the motion of the device ceases. The determination as to whether the mobile device returns within the threshold distance can,

similar to above, be calculated by determining a proximity of the mobile device to the person of the user. In such embodiments, the determination as to whether the mobile device returns to the person of the user can be effectuated by the retrieval, using the mobile device, of biometric signals related to the user such as gait, sound, and/or any other suitable biometric user-identifying signals.

[0044] In some embodiments, the flagging of the anomalous device condition may include providing a visual indication on the mobile device of the occurrence of the anomalous device condition.

[0045] In certain embodiments, the anomalous device condition may correspond to installation of a snooping application on the mobile device. This may occur during the confiscation of the device.

[0046] In some embodiments, the anomalous device condition may correspond to installation of a wire-tapping application, text-intercepting or e-mail intercepting application (or hardware device) installed on the mobile device. This may occur during the confiscation of the device.

[0047] A mobile device performance review application may be implemented for determining whether a current device performance status indicates the past occurrence of the anomalous device condition. For example, if the mobile device performance review application determines the past occurrence of the anomalous device condition, the application may query whether the anomalous device condition occurred between the start device confiscation time and the end device confiscation time.

[0048] Illustrative embodiments of apparatus and methods in accordance with the principles of the invention will now be described with reference to the accompanying drawings, which form a part hereof. It is to be understood that other embodiments may be utilized and structural, functional and procedural modifications may be made without departing from the scope and spirit of the present invention.

[0049] The drawings show illustrative features of apparatus and methods in accordance with the principles of the invention. The features are illustrated in the context of selected embodiments. It will be understood that features shown in connection with one of the embodiments may be practiced in accordance with the principles of the invention along with features shown in connection with another of the embodiments.

[0050] Apparatus and methods described herein are illustrative. Apparatus and methods of the invention may involve some or all of the features of the illustrative apparatus and/or some or all of the steps of the illustrative methods. The steps of the methods may be performed in an order other than the order shown or described herein. Some embodiments may omit steps shown or described in connection with the illustrative methods. Some embodiments may include steps that are not shown or described in connection with the illustrative methods, but rather shown or described in a different portion of the specification.

[0051] One of ordinary skill in the art will appreciate that the steps shown and described herein may be performed in other than the recited order and that one or more steps illustrated may be optional. The methods of the above-referenced embodiments may involve the use of any suitable elements, steps, computer-executable instructions, or computer-readable data structures. In this regard, other embodiments are disclosed herein as well that can be partially or wholly implemented on a computer-readable medium, for example, by storing computer-executable instructions or modules or by utilizing computer-readable data structures.

[0052] FIG. **1** is a schematic diagram of a mobile device **102** in accordance with the principles of the disclosure. Mobile device **102** preferably includes a screen **104**.

[0053] FIG. **2** is another schematic diagram of a mobile device **202** in accordance with the principles of the disclosure. Mobile device **202** preferably includes a memory **204**, a CPU **206**, and a device clock **208**. It should be noted that each of the components described herein should preferably be in electronic communication with one another.

[0054] FIG. **3** is a timing diagram of a mobile device clock in accordance with the principles of the disclosure. Temporary confiscation **302** shows a timeline of an exemplary confiscation that may occur in the setting of a domestic foreign airport or a domestic or foreign customs office. A device clock timeline is shown at **304**. The device clock **304** shows activation of the confiscation time capture at time T_0 and de-activation of the confiscation time capture T_1. Activation at T_0 and de-activation at T_1 set the confiscation time capture **306** between T_0 and T_1. All of this information can be based on activation and de-activation of device clock **304**.

[0055] In addition, device clock **304** may be monitored to determine whether device clock **304** has either markedly slowed down or markedly speeded up during the confiscation. One or more of such marked changes in the operation of device clock **304** may, under certain circumstances, indicate tampering.

[0056] FIG. **4** are timing diagrams of an exemplary network traffic monitor **402** and an exemplary bandwidth usage monitor **404** in accordance with the principles of the disclosure. It should be noted that information derived from either of network traffic monitor **402** and the bandwidth usage monitor **404** may be used to determine whether an anomalous event occurred during confiscation time capture **406**.

[0057] Network traffic monitor **402** shows an exemplary traffic in/traffic out analysis. This information may be used to determine whether improper information, as characterized by a relatively high level of network activity, was transmitted or received during confiscation time capture **406**.

[0058] Bandwidth usage monitor **404** shows use of bandwidth capacity during confiscation time capture **406**. It should be noted that a threshold level **412** may be presented in order to enable systems and/or methods according to the disclosure to quantify bandwidth usage and what may be considered an anomalous condition during the confiscation time capture **406**.

[0059] FIG. **5** is a timing diagram of a central processing unit (CPU) usage monitor **502** in accordance with the principles of the disclosure. It should be noted that a threshold level **512** may be presented in order to enable systems and/or methods according to the disclosure to quantify CPU usage and to classify what may be considered an anomalous condition during the confiscation time capture **506**.

[0060] FIG. **6** is a schematic diagram of memory **608** for use in systems and/or methods in accordance with the principles of the disclosure. At **606**, central I/O shows a connection to memory **608**. Within memory **608**, there may also be a signature lock-down file **602**.

[0061] Signature lock-down file **602** may preferably be a pre-confiscation image file. Such a file **602** may preferably be sealed off from the rest of memory by a hardware or

software lock at **604**. This lock protects the I/O to the signature lock-down file. This lock may be opened by input of a biometric characteristic associated with the user. This lock may be opened by unique identifier known to, and input by, the user. This lock may be opened by a one-time password transmitted to the user using a communication channel other than the mobile device associated with the user. This lock may be opened by a one-time password transmitted to the user using a communication channel which forms part of the mobile device. This lock may be opened by a combination of more than one of the biometric identifier, the password the OTP, or any other suitable secure information.

[0062] FIG. **7** is another schematic diagram of memory for use in systems and/or methods in accordance with the principles of the disclosure. FIG. **7** is similar to FIG. **6** in that memory **708**, central I/O **706** and lock **704** correspond to like elements in FIG. **6**. In contrast to FIG. **6**, FIG. **7** does illustrate graphically that image **702** is a hard-wired pre-travel image that may be relied on, post-tampering and post-reimaging, to return the device to its pre-travel image.

[0063] FIG. **8** is a mobile device **802** having a housing **802**, a screen **804**, a port **806** and a toggleable switch **808**. Switch **808** may preferably be used to lock port **806**. For the purposes of this application the term "lock" may be understood to mean preventing operation of port **806** such that electronic communications cannot pass through port **806**. As such, all attempts at tampering through locked port **806** would not be successful because no electronic communications would be allowed to pass through port **806**.

[0064] Switch **808**, or any other suitable actuation device, may be used by a user to lock port **806**. In certain embodiments, toggling of switch **808** may obtain an on/off toggle of port **806** only when switch **808** is toggled in a pre-determined pattern. As such, indeterminate, non-pattern, toggling of switch **808** will not obtain any change of the operability of port **806**.

[0065] FIG. **9** shows a mobile device having a housing **902**, a screen **904**, a port **906**, an optional port block indicator **912**, and a remote port toggling device **908**. Wireless signal indicators are shown at **910**.

[0066] Port **906** may be a wirelessly-lockable device. As such, port **906** may be locked remotely—e.g., by a wireless signal **910** generated by device **908**. For example, when the mobile device is confiscated, the user can use device **908** to generate a wireless locking signal **910**—thereby locking port **906** from tampering. Furthermore, some embodiments of the invention may also include a port block indicator **912** that indicates that port **906** is blocked.

[0067] Thus, systems and methods involving trusted travel devices have been provided. Persons skilled in the art will appreciate that the present invention can be practiced by other than the described embodiments, which are presented for purposes of illustration rather than of limitation.

What is claimed is:

1. A mobile device comprising enhanced travel security features, the mobile device comprising:

a memory;

a settable time clock, said time clock that operates to store a start device confiscation time in the memory and to store an end device confiscation time in the memory;

at least one monitor device selected from the group consisting of a:

a network traffic monitor device;

a bandwidth usage monitor device; and

a central processing usage monitor device;

wherein the at least one monitor device records the activity between the start device confiscation time and the end device confiscation time in the memory; and

wherein the at least one monitor device is configured to flag an anomalous device condition that occurred between the start device confiscation time and the end device confiscation time.

2. The mobile device of claim **1**, wherein at least one of the start device confiscation time and the end device confiscation time is determined by user command.

3. The mobile device of claim **1**, wherein the start device confiscation time is fixed and recorded when the mobile device passes a threshold distance from the mobile device user and the end device confiscation time is fixed and recorded when the mobile device returns within the threshold distance of the user.

4. The mobile device of claim **3**, wherein whether the mobile device passes the threshold distance is determined, at least in part, by calculating a distance between the mobile device and a second mobile device located on the user.

5. The mobile device of claim **3**, wherein whether the mobile device passes the threshold distance is determined, at least in part, by calculating a travel time following removal of the mobile device from the person of the user until the motion of the device ceases.

6. The mobile device of claim **5**, wherein the determination as to whether the mobile device returns within the threshold distance is calculated by determining a proximity of the mobile device to the person of the user.

7. The mobile device of claim **1** wherein the flagging of the anomalous device condition comprises providing a visual indication on the mobile device of the occurrence of the anomalous device condition.

8. The mobile device of claim **1** wherein the anomalous device condition corresponds to installation of a snooping application on the mobile device.

9. The mobile device of claim **1** wherein the anomalous device condition corresponds to installation of a wire-tapping application on the mobile device.

10. The mobile device of claim **1** further comprising a mobile device performance review application for:

determining whether a current device performance status indicates the past occurrence of the anomalous device condition, and,

if the mobile device performance review application determines the past occurrence of the anomalous device condition, querying whether the anomalous device condition occurred between the start device confiscation time and the end device confiscation time.

11. A method comprising enhancing travel security features associated with a mobile device, the method comprising:

operating a time clock on the mobile device, said operating comprising retrieving and storing a start device confiscation time in the memory and retrieving and storing an end device confiscation time in the memory;

monitoring the operation of the mobile device between the start device confiscation time and the end device confiscation time, said monitoring to determine the existence of an anomalous device condition, said monitoring comprising using one of:

a network traffic monitor device;
a bandwidth usage monitor device;
a battery performance monitor device;
a website presentation monitor device; and
a central processing usage monitor device;

wherein the monitoring records the activity between the start device confiscation time and the end device confiscation time in the memory; and

flagging the anomalous device condition that occurred between the start device confiscation time and the end device confiscation time.

12. The method of claim **11**, wherein at least one of the start device confiscation time and the end device confiscation time is determined by user command.

13. The method of claim **11**, further comprising fixing and recording the start device confiscation time when the mobile device passes a threshold distance from the mobile device user and fixing and recording the end device confiscation time when the mobile device returns within the threshold distance of the user.

14. The method of claim **13** further comprising determining the threshold distance, at least in part, by calculating a distance between the mobile device and a second mobile device located on the user.

15. The method of claim **13** further comprising determining the threshold distance, at least in part, by calculating a travel time following removal of the mobile device from the person of the user until the motion of the device ceases for a pre-determined amount of time.

16. The method of claim **15** further comprising determining whether the mobile device returns within the threshold distance by calculating a proximity of the mobile device to the person of the user.

17. The method of claim **11** wherein the flagging the anomalous device condition further comprises providing a visual indication on the mobile device of the occurrence of the anomalous activity.

18. The method of claim **11** wherein the anomalous activity corresponds to installation of a snooping application on the mobile device.

19. The method of claim **11** wherein the anomalous activity corresponds to installation of a wire-tapping application on the mobile device.

20. The method of claim **11** further comprising executing a post-confiscation time application for determining whether the anomalous activity occurred between the start device confiscation time and the end device confiscation time.

* * * * *