



- (51) **International Patent Classification:**
G06F 21/76 (2013.01) *G06F 21/50* (2013.01)
G06F 21/70 (2013.01)
- (21) **International Application Number:**
PCT/US2015/028248
- (22) **International Filing Date:**
29 April 2015 (29.04.2015)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (71) **Applicant:** HEWLETT PACKARD ENTERPRISE DEVELOPMENT LP [US/US]; 11445 Compaq Center Drive West, Houston, TX 77070 (US).
- (72) **Inventor:** LEWIS, John M.; 1160 Enterprise Way, Sunnyvale, California 94089 (US).
- (74) **Agents:** POSSETT, Ramya et al.; Hewlett Packard Enterprise, 3404 E. Harmony Road, Mail Stop 79, Fort Collins, CO 80528 (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, DK, DM,

DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

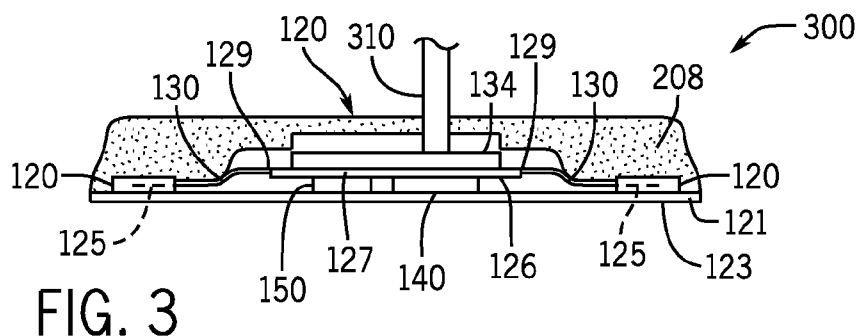
Declarations under Rule 4.17:

- as to the identity of the inventor (Rule 4.17(i))
- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))

Published:

- with international search report (Art. 21(3))

(54) **Title:** INHIBITING A PENETRATION ATTACK



(57) **Abstract:** A technique includes providing a security monitor to at least detect a penetration attack on a circuit assembly that contains the security monitor. The technique includes inhibiting success of the penetration attack, including flexibly mounting the security monitor to the circuit assembly to allow the security monitor to move in response to the security monitor being contacted during the penetration attack.

INHIBITING A PENETRATION ATTACK

Background

[0001] A given computer system (a data center, for example) that processes and/or stores sensitive data typically employs measures to protect the data from unauthorized access. For example, the computer system may process and/or store such sensitive information, as credit cardholder data, patient records, personnel information, intellectual property, and so forth.

[0002] The protective measures may guard against unauthorized access while the sensitive data is in motion (while the data is being communicated across communication channels, for example). For example, the computer system may encrypt data that is communicated across communication channels. The protective measures may further guard against access to cryptographic keys that are stored by the computer system and used by the system to encrypt/decrypt the sensitive data.

Brief Description of the Drawings

[0003] Fig. 1A is a perspective view of a secure key manager according to an example implementation.

[0004] Fig. 1B is a top view of a circuit assembly of the secure key manager according to an example implementation.

[0005] Fig. 2 is a cross-sectional view of the circuit assembly taken along line 2-2 of Fig. 1B according to an example implementation.

[0006] Fig. 3 is a cross-sectional view of the circuit assembly illustrating, in conjunction with Fig. 2, movement of a daughter card of the assembly during a punch through attack.

[0007] Fig. 4 is a flow diagram depicting a technique to inhibit a penetration attack according to an example implementation.

[0008] Fig. 5 is a schematic diagram illustrating a data center according to an example implementation.

[0009] Fig. 6 is a schematic diagram illustrating an architecture of the secure key manager according to an example implementation.

Detailed Description

[0010] An electronic system that processes and/or stores sensitive data (data representing patient records, personnel records, credit cardholder information, banking information, intellectual property, and so forth) may encrypt and decrypt the sensitive data while in transit. In this manner, the electronic system may communicate encrypted, sensitive data for internal communications within the electronic device (communications between the system's processing cores and memories, for example), as well as communicate encrypted, sensitive data in external communications between the system and other electronic systems.

[0011] For the purpose of encrypting and decrypting the sensitive data, the electronic system may use one or multiple cryptographic keys, called "security keys" herein. In this manner, the electronic system may store the security keys in one or more protected memories of the system. Because access to the security keys allows access to the underlying sensitive data, the electronic system may have a physical security barrier to prevent, or at least inhibit, unauthorized access to the stored security key(s). For example, sensitive components of the electronic system, which store security keys, may be enclosed by a locked, metal container, which forms at least part of a physical security barrier to guard against unauthorized access to the stored keys. In this manner, the metal enclosure may have no open ports through which a tool (a probe, a punch through device, and so forth) may be inserted for such purposes as sensing electrical signals (representing the keys, for example), physically extracting memory storing security keys, and so forth.

[0012] The electronic system may still be vulnerable to a "penetration attack," even when enclosed in a metal container. A penetration attack is a physical attack on an electronic system in which a tool is used to penetrate the system's physical security barrier (such as a metal container) for purposes of gaining access to information (such as one or multiple security keys) that is stored in the system. For example, the tool may contain a drill or punch to form a hole in the metal container (and/or other enclosure or security barrier) of the electronic system, and a probe may be inserted into the hole to sense one or multiple electrical signals of the electronic system for

purposes of retrieving the security key(s). Another type of penetration attack, called a "punch through attack" herein, employs a tool to penetrate into integrated circuits of the electronic system for purposes of extracting memory-containing circuitry and reading any data stored therein.

[0013] For purposes of thwarting a penetration attack, the electronic system may contain one or multiple penetration detection boundaries. The penetration boundary(ies) allow the electronic system to detect an ongoing penetration attack, so that the electronic system may timely take corrective action. In this regard, when a penetration attack is detected, the electronic system may take such actions as alerting a system administrator; alerting security personnel; erasing security keys before the keys are extracted; power off or shutting down operations of the electronic system, and so forth.

[0014] A given penetration detection boundary may be formed from one or multiple traces in one or multiple metal layers of a circuit substrate (a printed circuit board substrate (PCB), for example). The trace(s) are arranged in pattern(s) so that when a penetration attack occurs, which penetrates the circuit substrate, at least one trace is broken. Due to signal interruption(s) caused by the broken trace(s), the electronic system is alerted to the attack. More specifically, the electronic system may contain a circuit called a "security monitor" herein, which may be coupled to penetration detection traces to detect a signal interruption that indicates a penetration attack.

[0015] The security monitor may be unable to respond quickly enough during a penetration attack to prevent sensitive information from being extracted from the electronic system. For example, a punch through attack may punch out, or remove, memory-containing circuitry from the electronic system before the system has time to undertake operations to erase sensitive data stored in the circuitry. Moreover, a punch through attack may disable the security monitor before the security monitor can respond.

[0016] Systems and techniques are disclosed herein, which provide additional time for a security monitor to respond to a penetration attack, such as a punch through attack. In particular, in accordance with example implementations, the security

monitor is mounted on a circuit substrate assembly, referred to as a "daughter card" herein; and the daughter card, is flexibly mounted to another circuit substrate called a "base card" herein. The flexible mounting of the daughter card to the base card creates a spring-like cushion, which allows the daughter card to move if the card is contacted with a tool during a punch through attack. In this manner, because the flexible mounting allows the daughter card to move with the punch through tool, the punch through tool is at least momentarily unable to penetrate circuitry of the daughter card when the tool first contacts the card. Although the punch through tool may be able to penetrate the daughter card after the tool eventually presses the daughter card into the base card, a time delay is created between the time of initial contact and the time that penetration occurs. Therefore, additional time is created for the security monitor to successively take and complete corrective action to prevent the punch through attack from being successful.

[0017] Referring to Fig. 1A, as a more specific example, an electronic system (a processor-based data center, for example) may contain one or multiple secure key managers, such as example secure key manager 100, for purposes of managing, protecting, serving and preserving security keys for the system. The secure key manager 100 may, in accordance with example implementations, be a blade that is constructed to be received in a backplane bus slot of a computer system rack.

[0018] The secure key manager 100 may have one or multiple physical security barriers that protect the sensitive components of the manager 100 against a penetration attack. For example, as depicted in Fig. 1A, the secure key manager 100 may have an outer metal enclosure 110 that surrounds, or encloses, a circuit board assembly 120. The circuit board assembly 120 contains various integrated circuits (ICs) that, in general, perform the functions of the secure key manager 100 and store sensitive information (security keys, data encrypted by security keys, and so forth) for the manager 100.

[0019] In accordance with example implementations, the metal enclosure 110 may, in general, have no ports, or openings, through which a penetration attack may occur (through which a punch through tool or probe may be inserted, for example) for

purposes of gaining access to the security key(s) and/or other sensitive information stored inside the secure key manager 100. The secure key manager 100 may communicate with external circuitry using (as examples) connector sockets, optical signaling, inductive coupling connections, and so forth. The metal enclosure 110 may include various security mechanisms, such as (as an example) key locks 112, which secure the enclosure 110 from being opened (by removal of a front panel 111 of the enclosure 110, for example) except when two keys (keys held by two authorized employees, for example) are concurrently inserted and turned.

[0020] Referring to Fig. 1B, in accordance with an example implementation, the circuit board assembly 120 includes a base circuit board substrate assembly 121, called a "base card 121" herein. As an example the base card 121 may include a circuit substrate 123, such as a printed circuit board (PCB), and various ICs may be mounted on the upper surface of the substrate (for the orientation of the circuit board assembly 120 depicted in Fig. 1B). One or multiple ICs of the base card 121 may contain a memory that stores sensitive information for the secure key manager 100.

[0021] The circuit substrate 123, in accordance with example implementations, is a multiple layer substrate, which contains metal layers and intervening insulating layers. One or multiple metal layers of the circuit substrate 123 may contain traces for purpose of routing signals, power and ground for the ICs of the base card 121.

[0022] Moreover, one or multiple metal layers of the circuit substrate 123 may contain one or multiple traces that are patterned to form a penetration detection boundary of the secure key manager 100. In this manner, the penetration detection boundary is constructed to provide an indication to the secure key manager 100 when a penetration attack at least partially penetrates the circuit substrate 123.

[0023] More specifically, in accordance with example implementations, the secure key manager 100 contains a circuit called a "security monitor 134," which is electrically coupled to the traces of the penetration boundary of the base card 121 for purposes of being alerted when a penetration attack or attempted penetration attack through/into the circuit substrate 123. In this manner, the security monitor 134 monitors the traces of the base card's penetration detection boundary for purposes

of detecting when a signal interruption (indicative of a penetration attack through the substrate 123) occurs. In particular, the penetration detection boundary of the base card 121 is positioned to alert the security monitor 134 when a penetration attack (more specifically, a "punch through attack") originating from a region below the base card 121 (for the orientation depicted in Fig. 1B) occurs. The security monitor 134 may also be coupled to a penetration detection boundary that provides an alert for a penetration attack that originates from a region above the base card 121 (for the orientation depicted in Fig. 1B). In this manner, the circuit board assembly 121 may be covered with another circuit board substrate (a flexible circuit substrate, for example), which is not shown in Fig. 1B. This other circuit board substrate contains a penetration detection boundary and is electrically coupled (via at least one connector, not shown) to the security monitor 134, in accordance with example implementations.

[0024] In accordance with example implementations, the security monitor 134 is disposed on a circuit board substrate assembly 126, called a "daughter card 126" herein. As depicted in Fig. 1B, the daughter card 126 may be smaller than the base card 121; the security monitor 134 may be mounted to a circuit substrate 127 (a PCB substrate, for example) of the daughter card 126; and the security monitor 134 may, in general, occupy most of the upper surface area of this circuit board substrate 127. The circuit substrate 127 may, in general, be a multiple layer substrate, which contains metal layers and intervening insulating layers.

[0025] One or multiple metal layers of the circuit substrate 127 may contain traces for purpose of routing signals, power and ground for the ICs of the daughter card 126, such as the security monitor 134 as well as other circuitry described herein. Moreover, one or multiple metal layers of the circuit substrate 127 may contain traces that form a penetration detection boundary, which may be electrically coupled to the security monitor 134.

[0026] In accordance with example implementations, the daughter card 126 is not rigidly mounted to the base card 121. Rather, in accordance with example implementations, the daughter card 126 contains one or multiple flexible connections

that mechanically and electrically couple the daughter card 126 to the base card 121. For the specific implementation that is depicted in Fig. 1B, two flexible connections mechanically and electrically couple the daughter card 126 to the base card 121. As an example, a given flexible connection may be formed from a flexible printed circuit substrate, or flexible circuit 130 (also called a "flex circuit"), which has ends 125 and 129 that terminate on the base card 121 and daughter card 126, respectively.

[0027] As a more specific example, in accordance with some implementations, the end 125 of the flexible circuit 130 may terminate in a connector 124 that is disposed on the base card 121. As examples, the connector 124 may be a zero insertion force (ZIF), a low insertion force (LIF) connector, a surface mount connector or a through hole connector. Other connectors may be used, in accordance with further example implementations. In general, the end 125 of the flexible circuit 130 is secured, or mechanically held, by the connector 124, and electrical traces of the flexible circuit 130, which extend into the end 125 form electrical connections with electrical contacts of the connector 124. The opposite end 129 of the flexible circuit 130 may likewise terminate in a connector (not shown) that is mounted to the daughter card 126, such as a ZIF, LIF, surface mount or through hole connector, as examples.

[0028] Fig. 2 depicts a cross-sectional view of the circuit assembly 120 of Fig. 1B, with the addition of potting material 208. The potting material 208 may be, as an example, an electrically nonconductive, insulating, gel, epoxy or other material, which coats the upper surface of the circuit assembly 120. The secure key manager 100 may not include potting material, in accordance with further example implementations. As depicted in Fig. 2, the flexible circuits 130 have sufficient respective lengths to suspend the daughter card 126 over the base card 121. In this manner, as depicted in Fig. 2, a clearance, or gap G, exists between the bottommost surface of the daughter card 126 and the uppermost surface of the base card 121.

[0029] The gap G, in combination with the flexible nature of the circuits 130, creates a spring-like cushion that allows the daughter card 126 to move if the daughter card 126 is contacted by a tool from above during a punch through attack. This

movement, in turn, momentarily prevents the daughter card 126 from exerting a sufficient reaction force on the tool, which would otherwise allow the tool to punch into the card 126 (and possibly extract memory circuitry of the card 126, for example).

[0030] More specifically, referring to Fig. 3 in conjunction with Fig. 2, when contacted by a tool 310 from above during a punch through attack, the daughter card 126 moves with the tool 310 until the tool 310 presses the daughter card 126 firmly against the base card 121. When the tool 310 is able to press the daughter card 126 against the base card 121, the tool 310 may be able to punch into the card 126 and possibly extract memory circuitry of the card 126 (by extracting the circuitry through a hollow point of the tool 310, for example). However, due to the flexible mounting of the daughter card 126 to the base card 121, a delay is created between the time when the tool 310 first contacts the daughter card 126 and the time at which punch out of a portion of the card 126 may occur. Therefore, even if the punch through attack succeeds in extracting circuitry from the daughter card 126, the security monitor 134 has additional time created by flexible mounting of the daughter card 126 to take corrective action. In this manner, the additional time may allow the security monitor 134 to erase sensitive information (keys, encrypted data and so forth) before memory circuitry of the security monitor 134 (or of another component) is extracted and/or before the security monitor 134 is disabled due to the punch through attack.

[0031] In accordance with example implementations, the security monitor 134 contains one or multiple memories that store sensitive data for the secure key manager 100. Therefore, in response to detecting a penetration attack, the security monitor 134 may erase its own memory contents. Moreover, in accordance with example implementations, the security monitor 134 may erase the memory contents (via communications or signaling) of other devices of the secure key manager 100, when a penetration attack is detected.

[0032] Referring to Fig. 4, to summarize, in accordance with example implementations, a technique 400 includes providing (block 404) a security monitor

to at least detect a penetration attack on a circuit assembly that contains the security monitor. The technique 400 includes inhibiting (block 408) a penetration attack, including flexibly mounting the security monitor to the circuit assembly to allow the security monitor to move in response to the security monitor being contacted during the penetration attack.

[0033] In accordance with example implementations, the daughter card 126 may have features that create additional time for the security monitor 124 to respond to a punch through attack (in addition to the time created by the flexible mounting of the daughter card 126 to the base card 121). In this manner, referring to Fig. 2, in accordance with example implementations, the security monitor 134 is mounted on top surface of the circuit substrate 127 of the daughter card 126, and energy storage circuits 140, 150 and 152 are mounted on the bottom surface of the circuit substrate 127. The energy storage circuits 140, 150 and 152 provide temporary power for memory-containing circuitry of the security monitor 134, which might be removed in a punch through attack.

[0034] More specifically, when the circuit assembly 120 is intact, the circuit components (the security monitor 134, energy storage circuits 140, 150, 152, and so forth) of the daughter card 126 receive electrical power through electrical conductors of one or both flexible circuits 130. In this manner, the electrical conductors may be voltage supply and ground rails that communicate electrical power from power supply/distribution circuitry that is disposed on the base card 121 to the circuit components of the daughter card 126. The energy storage circuits 140, 150 and 152 receive the power from the base card 121 and store energy in response thereto. As an example, the energy storage circuits 140, 150 and 152 may include spatially distributed arrays of capacitors that are charged from the power that is communicated from the base card 121; and the security monitor 134 may be an integrated circuit package, such as a microprocessor core-based package. In accordance with further example implementations, the energy storage circuit 140, 150 or 152 may include one or multiple devices that store energy other than capacitors, such as (as examples) electrochemical cells and flat batteries.

[0035] In accordance with example implementations, the energy storage circuits 140, 150 and 152 are disposed directly beneath associated circuits of the security monitor 134, which are independently autonomous and perform important functions for the security monitor 134, such as processor core circuits containing memories and other memory-containing autonomous circuits, for example. Moreover, vias of the circuit substrate 127 of the daughter card 126 electrically couple the energy storage circuits 140, 150 and 152 to the power supply terminals of their associated circuits of the security monitor 134. Therefore, in the event that a punch through attack removes one of these circuits of the security monitor 134, there is a relatively high likelihood that its associated temporary memory storage, located directly beneath, is also removed. As a result, even though a given circuit may be removed from the daughter card 126 in a punch through attack, the circuit receives power for an additional time after its removal, thereby allowing the circuit time to respond to the attack (e.g., additional time is created to allow the extracted circuit to erase its associated memory contents, for example).

[0036] It is noted that the daughter card 126 may have circuit components, other than/in addition to the security monitor 134 and energy storage circuits 140, 150 and 152, in accordance with further example implementations. Moreover, in accordance with further example implementations, the daughter card 126 may have more than three or less than three energy storage circuits.

[0037] Referring Fig. 5, in accordance with example implementations, the secure key manager 100 may be part of a data center 500, in which the secure key manager 100 manages, stores and serves keys for one or multiple clients 504 of the data center 500. As an example, the secure key manager 100 and clients 504 may be blades that are inserted into one or more racks of the data center 500.

[0038] In accordance with example implementations, the secure key manager 100 may have an architecture that is schematically represented in Fig. 6. Referring to Fig. 6, in general, the secure key manager 100 may include hardware 602 and machine executable instructions, or "software," 650. In general, the hardware 602 may include one or multiple central processing unit (CPU) cores 606. In accordance

with example implementations, the security monitor 134 (see Fig. 2) may include one or multiple CPU cores 606; and in accordance with example implementations, one or multiple CPU cores 606 of the security monitor 134 may have an associated energy storage circuit disposed beneath the core 606, as described above. In accordance with example implementations, a given CPU core 906 may include onboard memory, such as level one (L1) cache 608 and a level two (L2) cache 610; and sensitive data (keys and so forth) may be stored in one or both caches 608 and 610.

[0039] The hardware 602 may also include memory that is accessed by the CPU core(s) 606, such as a level three (L3) cache 612 and a system memory 616. In accordance with an example implementation, sensitive data may be stored in the L3 cache 612 and/or system memory 616; and a given energy storage circuit may be disposed between circuitry containing the memory 616, L3 cache 616 and at least one of the processor cores 606.

[0040] The hardware 602 may include other and/or different components than the components that are depicted in Fig. 6 in further example implementations, such as a memory controller 614, a network interface 618, and so forth.

[0041] The software 650 may include a set of machine executable instructions that, when executed by one or multiple CPU core(s) 606, cause the CPU core(s) 606 to form a secure key manager engine 652 to manage, serve and protect keys as well as perform various cryptographic ciphers. The software 650 may include a set of machine executable instructions that, when executed by one or multiple CPU core(s) 606, cause the CPU core(s) 606 to form a security monitor engine 653 to perform one or multiple functions of the security monitor 134 (see Fig. 2), such as providing signals to penetration detection traces, receiving signals from the penetration detection traces to detect a penetration attack, taking corrective action in response to detecting a penetration attack, and so forth. The software 650 may include different and/or other machine executable instructions that when executed may form various other software components, such as an operating system 654, device drivers, applications and so forth.

[0042] Other implementations are contemplated, which are within the scope of the appended claims. For example, in accordance with further example implementations, a security monitor may be flexibly mounted to a circuit assembly in an electronic system other than a secure key manager and/or be part of a system other than a data center system.

[0043] It is noted that references herein to direction and orientation, such as "upper," "lower," top," "bottom," and so forth are used herein to describe the figures; and the substrates, circuit assemblies, cards, and so forth, may be used in a variety of orientations, depending on the particular implementation. For example, the circuit assembly 120, in accordance with example implementations, may be used in an orientation that is flipped over or turned on its inside, relative to the orientation that is depicted in Figs. 1B, 2 and 3.

[0044] While the present techniques have been described with respect to a number of embodiments, it will be appreciated that numerous modifications and variations may be applicable therefrom. It is intended that the appended claims cover all such modifications and variations as fall within the scope of the present techniques.

What is claimed is:

1 1. A method comprising:
2 providing a security monitor to at least detect a penetration attack on a circuit
3 assembly containing the security monitor; and
4 inhibiting success of the penetration attack, comprising flexibly mounting the
5 security monitor to the circuit assembly to allow the security monitor to move in
6 response to the security monitor being contacted during the penetration attack.

1 2. The method of claim 1, further comprising mounting the security
2 monitor on a first substrate, wherein mounting the security monitor to the circuit
3 assembly comprises mounting the first substrate to a second substrate of the circuit
4 assembly to suspend one of the first and second substrates relative to the other
5 substrate.

1 3. The method of claim 1, further comprising:
2 communicating power to circuitry of the security monitor through at least one
3 conductor; and
4 providing an energy storage circuit to provide temporary power to the circuitry
5 monitor in the event the penetration attack isolates the circuitry from receiving the
6 communicated power.

1 4. The method of claim 1, wherein inhibiting success of the penetration
2 attack further comprises:
3 in response to the security monitor detecting the penetration attack, using the
4 security monitor to take corrective action to the attack.

1 5. The method of claim 4, wherein using the security monitor to take
2 corrective action comprises:
3 erasing at least one security key stored on the circuit assembly.

1 6. An apparatus comprising:
2 an enclosure;
3 at least one penetration detection layer to detect a penetration attack directed
4 to a secure region inside the enclosure; and
5 an assembly disposed in the secure region, the assembly comprising:
6 a first circuit board;
7 second circuit board having associated circuitry comprising a security
8 monitor, the security monitor being coupled to the at least one penetration detection
9 layer to detect the penetration attack; and
10 a spring mount attached between the first and second circuit boards to
11 provide a delay between a time that the penetration attack contacts the second
12 circuit board and a time that the penetration attack removes at least part of the
13 circuitry associated with the second circuit board to allow the security monitor to
14 respond to the penetration attack to inhibit success of the attack.

1 7. The apparatus of claim 6, wherein the spring mount comprises a
2 flexible connector having a first end connected to the first circuit board and a second
3 end connected to the second circuit board.

1 8. The apparatus of claim 7, wherein:
2 the first circuit board comprises a power distribution circuit to provide a power
3 signal; and
4 the flexible connector communicates the power signal to the circuitry of the
5 second circuit board.

1 9. The apparatus of claim 8, further comprising an energy source
2 mounted to the second circuit board, wherein the energy source charges using the
3 power signal to provide a temporary source of power for the circuitry of the second
4 circuit board.

1 10. The apparatus of claim 7, wherein:
2 the first circuit board comprises a penetration detection layer to detect a
3 penetration attack occurring through the first circuit board; and
4 the flexible connector communicates at least one signal from the penetration
5 detection layer of the first circuit board to the security monitor.

1 11. The apparatus of claim 7, wherein the second circuit comprises at least
2 one metal layer comprising a penetration detection trace.

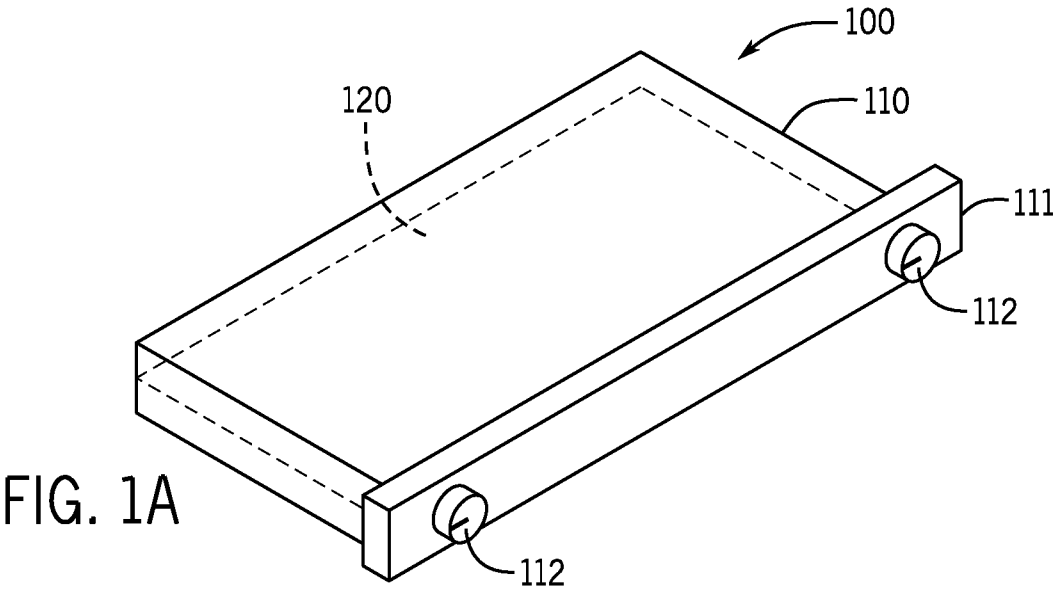
1 12. An apparatus comprising:
2 a first substrate;
3 a penetration attack monitoring circuit mounted to the first substrate, the
4 penetration attack monitoring circuit comprising a memory and the memory to store a
5 key;
6 a base substrate;
7 a flexible mounting to suspend the first substrate over the base substrate and
8 cause the first substrate to be pushed toward the base substrate in response to the
9 first substrate being contacted during a penetration attack,
10 wherein the penetration attack monitoring circuit detects the penetration
11 attack and takes corrective action in response thereto to inhibit the penetration attack
12 from revealing the key.

1 13. The apparatus of claim 12, wherein the penetration attack monitoring
2 circuit erases the key in response to detecting the penetration attack.

1 14. The apparatus of claim 12, further comprising a potting material to
2 cover the first substrate and the penetration attack monitoring circuit.

1

- 1 15. The apparatus of claim 12, wherein the base comprises a first set of at
2 least one penetration detection layer, the first substrate comprises a second set of at
3 least one penetration detection layer, and the penetration detection layers of the first
4 and second sets are electrically coupled to the penetration attack monitoring circuit.



2 / 4

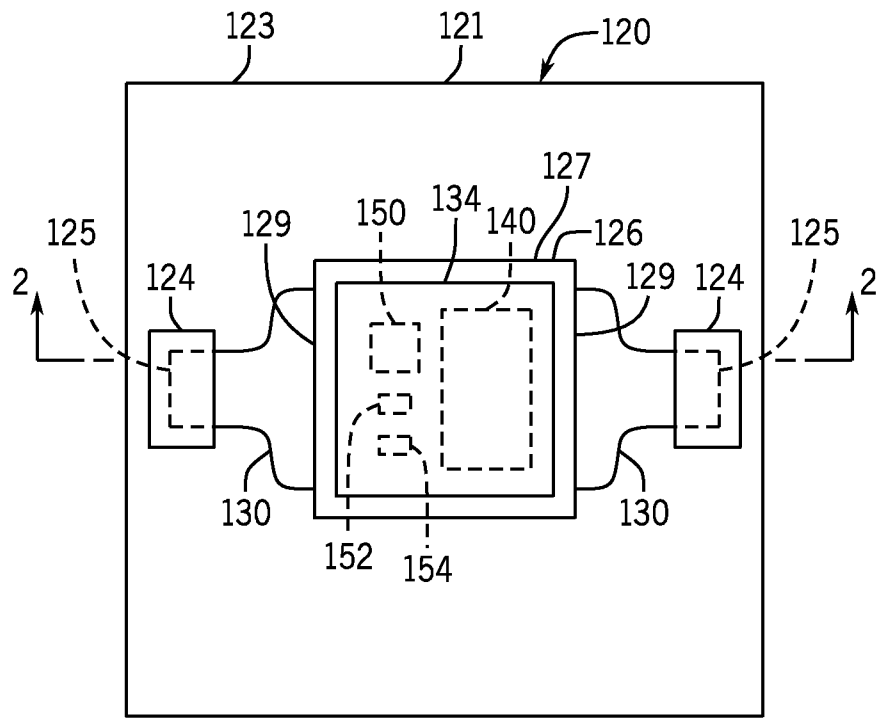


FIG. 1B

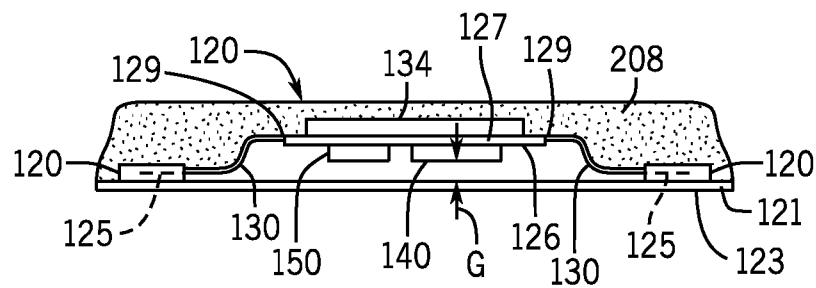


FIG. 2

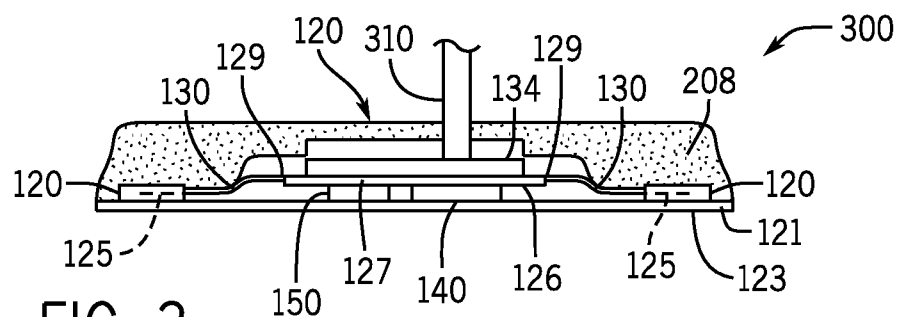


FIG. 3

3 / 4

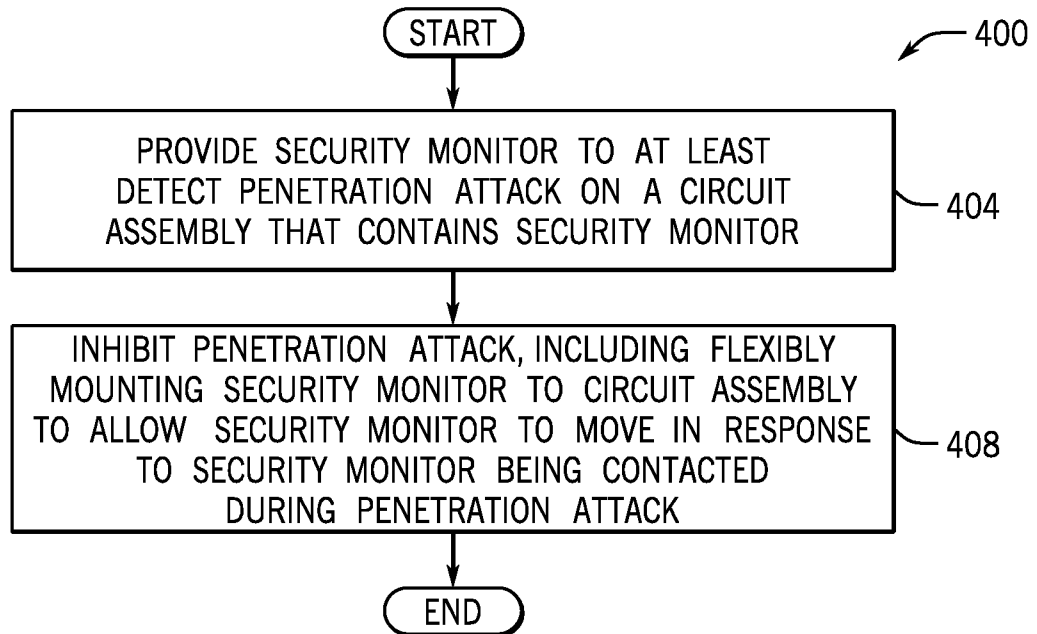


FIG. 4

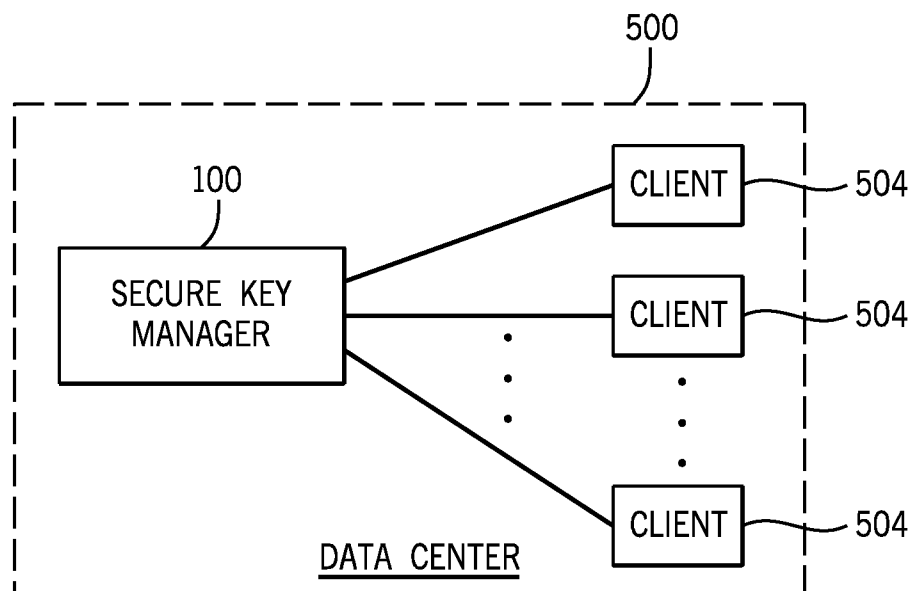


FIG. 5

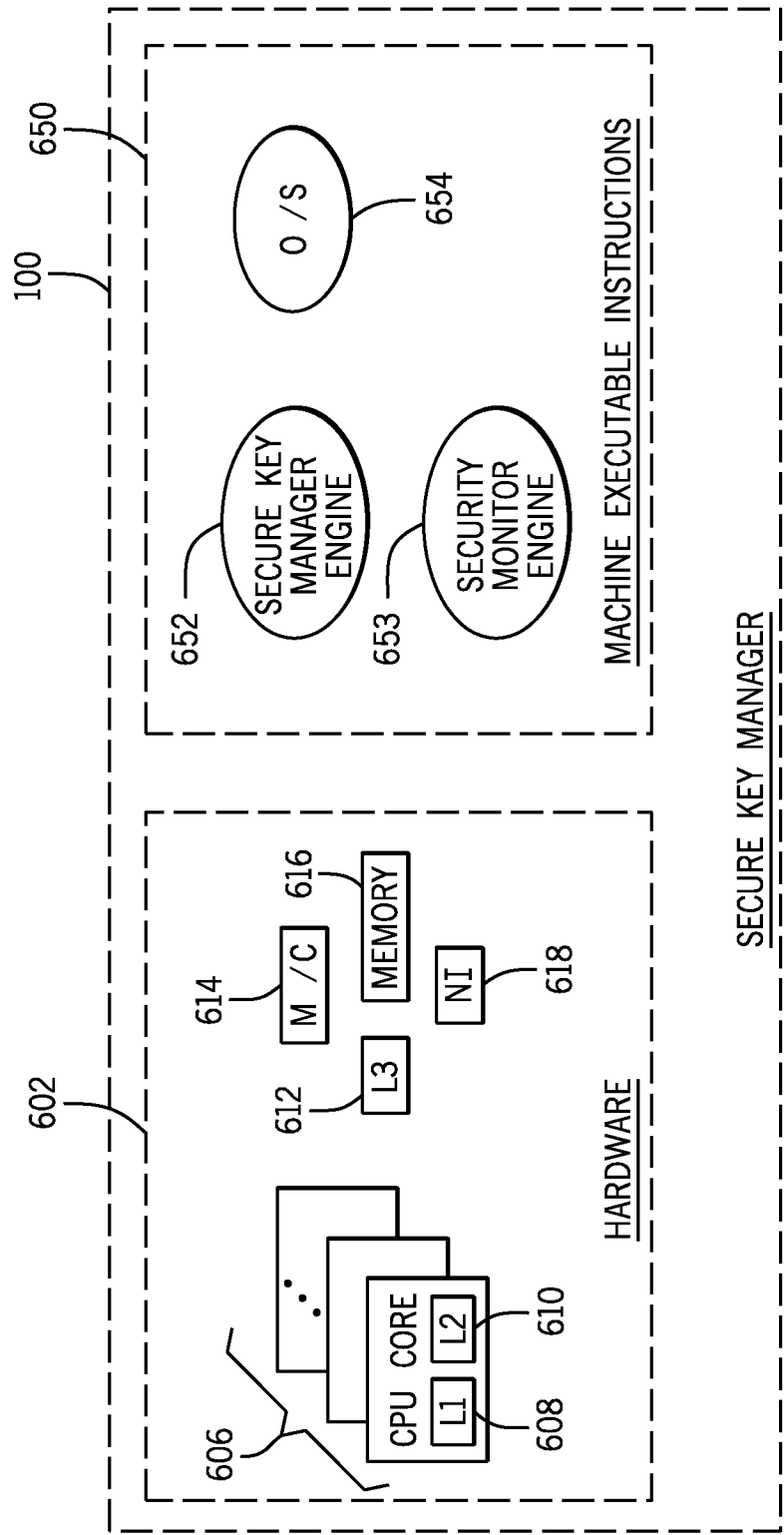


FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/028248**A. CLASSIFICATION OF SUBJECT MATTER****G06F 21/76(2013.01)i, G06F 21/70(2013.01)i, G06F 21/50(2013.01)i**

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/76; G08B 13/12; H05K 9/00; H01L 21/50; G07F 19/00; H04L 9/32; G06F 1/00; H01L 23/58; H05K 7/06; G06F 21/70; G06F 21/50

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: inhibiting, penetration attack, flexible, erasing, sensitive data, cover, substrate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2014-158159 A1 (HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.) 02 October 2014 See paragraphs [0018]-[0022], [0024]-[0027], [0029]-[0030]; claim 1; and figures 1-2, 4.	1-2, 4-5
Y		3, 6-15
Y	US 2010-0213590 A1 (ROBERT W. WARREN et al.) 26 August 2010 See paragraphs [0020]-[0021], [0027]-[0028], [0032]; claim 1; and figures 1, 2A-2B.	3, 6-15
A	EP 1045352 A1 (W L GORE & ASSOCIATES S.R.L.) 18 October 2000 See paragraphs [0026]-[0029]; and figure 1.	1-15
A	US 2002-0002683 A1 (JUSTIN H. BENSON et al.) 03 January 2002 See paragraphs [0050], [0065]-[0066]; and figures 2, 4.	1-15
A	US 7349223 B2 (JOSEPH MICHAEL HAEMER et al.) 25 March 2008 See column 21, line 59 - column 22, line 36; and figure 21.	1-15

☐ 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

25 February 2016 (25.02.2016)

Date of mailing of the international search report

25 February 2016 (25.02.2016)

Name and mailing address of the ISA/KR

International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701,
Republic of Korea

Facsimile No. +82-42-472-7140

Authorized officer

COMMISSIONER

Telephone No. +82-42-481-3578



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2015/028248

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2014-158159 A1	02/10/2014	None	
US 2010-0213590 A1	26/08/2010	US 8455990 B2	04/06/2013
EP 1045352 A1	18/10/2000	None	
US 2002-0002683 A1	03/01/2002	US 7054162 B2	30/05/2006
		WO 01-59544 A2	16/08/2001
		WO 01-59544 A3	20/06/2002
US 7349223 B2	25/03/2008	CN 101019473 A	15/08/2007
		CN 1575350 A	02/02/2005
		EP 1183604 A2	06/03/2002
		EP 1200843 A1	02/05/2002
		EP 1292834 A2	19/03/2003
		EP 1292834 B1	30/11/2005
		EP 1419285 A1	19/05/2004
		EP 1549962 A2	06/07/2005
		JP 2003-501819 A	14/01/2003
		JP 2003-506686 A	18/02/2003
		JP 2004-500699 A	08/01/2004
		JP 2004-501517 A	15/01/2004
		JP 2005-501179 A	13/01/2005
		JP 2006-507479 A	02/03/2006
		JP 2006-508495 A	09/03/2006
		JP 2007-538263 A	27/12/2007
		JP 2008-533441 A	21/08/2008
		JP 3794586 B2	05/07/2006
		KR 10-0707044 B1	13/04/2007
		KR 10-2002-0026585 A	10/04/2002
		KR 10-2002-0028159 A	16/04/2002
		KR 10-2004-0044459 A	28/05/2004
		KR 10-2004-0093740 A	08/11/2004
		KR 10-2005-0014885 A	07/02/2005
		KR 10-2007-0085122 A	27/08/2007
		KR 10-2007-0093450 A	18/09/2007
		US 2002-0171133 A1	21/11/2002
		US 2003-0099097 A1	29/05/2003
		US 2003-0214045 A1	20/11/2003
		US 2003-0218244 A1	27/11/2003
		US 2004-0008045 A1	15/01/2004
		US 2004-0022042 A1	05/02/2004
		US 2004-0075455 A1	22/04/2004
		US 2004-0223309 A1	11/11/2004
		US 2005-0003196 A1	06/01/2005
		US 2005-0026476 A1	03/02/2005
		US 2005-0042932 A1	24/02/2005
		US 2005-0051353 A1	10/03/2005
		US 2005-0068054 A1	31/03/2005

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2015/028248

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		US 2005-0275418 A1	15/12/2005
		US 2006-0119377 A1	08/06/2006
		US 2006-0186906 A1	24/08/2006
		US 2006-0240690 A9	26/10/2006
		US 2007-0046304 A1	01/03/2007
		US 2007-0057684 A1	15/03/2007
		US 2007-0098895 A1	03/05/2007
		US 2007-0144841 A1	28/06/2007
		US 2007-0245553 A1	25/10/2007
		US 2008-0090429 A1	17/04/2008
		US 2008-0246500 A1	09/10/2008
		US 2008-0297186 A1	04/12/2008
		US 2009-0153165 A1	18/06/2009
		US 2010-0066393 A1	18/03/2010
		US 6710609 B2	23/03/2004
		US 6791171 B2	14/09/2004
		US 6799976 B1	05/10/2004
		US 6812718 B1	02/11/2004
		US 6815961 B2	09/11/2004
		US 6917525 B2	12/07/2005
		US 7009412 B2	07/03/2006
		US 7126220 B2	24/10/2006
		US 7126358 B2	24/10/2006
		US 7137830 B2	21/11/2006
		US 7138818 B2	21/11/2006
		US 7153399 B2	26/12/2006
		US 7247035 B2	24/07/2007
		US 7382142 B2	03/06/2008
		US 7403029 B2	22/07/2008
		US 7579848 B2	25/08/2009
		US 7621761 B2	24/11/2009
		US 7772860 B2	10/08/2010
		US 7812626 B2	12/10/2010
		US 7872482 B2	18/01/2011
		US 7884634 B2	08/02/2011
		US 7952373 B2	31/05/2011
		WO 00-73905 A2	07/12/2000
		WO 00-73905 A3	07/09/2001
		WO 00-74110 A2	07/12/2000
		WO 00-74110 A3	27/09/2001
		WO 01-09623 A1	08/02/2001
		WO 01-98793 A2	27/12/2001
		WO 01-98793 A3	25/07/2002
		WO 03-18865 A1	06/03/2003
		WO 03-81725 A2	02/10/2003
		WO 03-81725 A3	18/12/2003
		WO 04-01807 A2	31/12/2003
		WO 2004-001807 A3	23/12/2004
		WO 2004-008492 A2	22/01/2004
		WO 2004-008492 A3	06/05/2004

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2015/028248

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		WO 2005-115068 A2	01/12/2005
		WO 2005-115068 A3	25/01/2007
		WO 2006-086512 A2	17/08/2006
		WO 2006-086512 A3	10/07/2008
		WO 2007-115053 A2	11/10/2007
		WO 2007-115053 A3	17/07/2008