

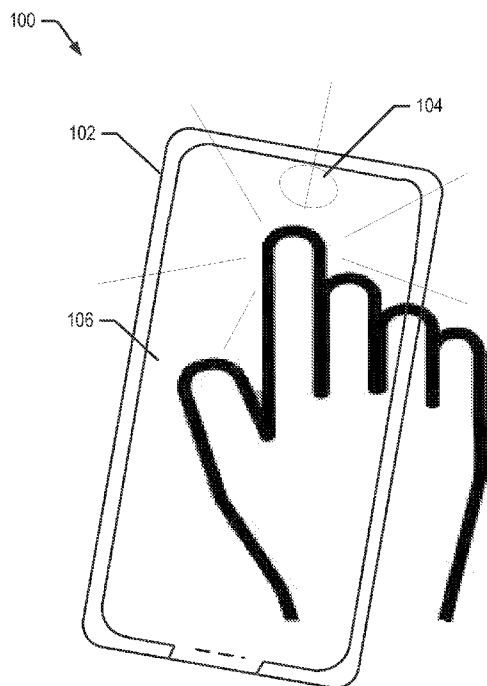


(43) International Publication Date
16 October 2014 (16.10.2014)

- (51) International Patent Classification:
G06F 21/00 (2013.01)
- (21) International Application Number:
PCT/US2014/033495
- (22) International Filing Date:
9 April 2014 (09.04.2014)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
61/811,191 12 April 2013 (12.04.2013) US
- (71) Applicant: UAB RESEARCH FOUNDATION [US/US];
701 S. 20th Street, Suite 1120G, Birmingham, Alabama
35294-0111 (US).
- (72) Inventors: SAXENA, Nitesh; 1374 Chapel Street, Hoover,
Alabama 35226 (US). SHRESTHA, Babins; 1121 14th
Ave S., Birmingham, Alabama 35205 (US).
- (74) Agent: MYERS BIGEL SIBLEY & SAJOVEC, P.A.;
P.O. Box 37428, Raleigh, North Carolina 27627 (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,

[Continued on next page]

(54) Title: DETECTING PHYSICAL GESTURES FOR MOBILE DEVICE SECURITY



(57) Abstract: A security check may correspond to a request for a resource on a mobile computing device. A security message is displayed on the computing device based on the security check. A proximity sensor signal generated in response to an action of an object proximate to a proximity sensor of the computing device is detected. The proximity sensor signal corresponds to the security message. Use of the resource is authorized based on the proximity sensor signal.

FIGURE 1



WO 2014/169036 A1



KZ, LA, LC, LK, LR, LS, LT, 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.

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).

Published:

(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, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,

- with international search report (Art. 21(3))
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

DETECTING PHYSICAL GESTURES FOR MOBILE DEVICE SECURITY**TECHNICAL FIELD**

[0001] The present disclosure relates generally to software applications, security and mobile computing devices.

BACKGROUND

[0002] Mobile devices, such as smartphones, watches and tablets, are incorporating more and more sensors and communication interfaces, which provide for much functionality that is not available to desktop computers. For example, many smartphones incorporate a Near Field Communication (NFC) chip, which allows short, paired transactions with other NFC-enabled devices in close proximity. The use of NFC-equipped devices as payment tokens is considered to be a next generation payment system.

[0003] Due to their popularity, mobile devices are becoming a target for malicious activities. There has been a rapid increase in malware targeting various mobile device platforms. After infecting a device, malware can gain access to sensitive resources or services for various purposes, such as stealing user data, making premium phone calls, sending messages, damaging the device, tracking user activities or location, or simply annoying the user. Newer functionalities, such as NFC, can make mobile devices a popular malware target for credential and credit card theft.

[0004] Due to resource constraints of mobile devices, such as limited battery power, existing malware defenses for desktop computers cannot typically be applied directly on the mobile device platform. Although some mobile devices employ permission models to prevent malware from being installed, this approach relies on user diligence and awareness, which users may lack in practice. Existing malware defenses, without

considering the special characteristics of mobile devices, may not be sufficient to detect sophisticated malware.

BRIEF SUMMARY

[0005] According some embodiments of the disclosure, it is determined that a security check corresponds to a request for a resource on a computing device. A security message is provided for display on the computing device based on the security check. A proximity sensor signal generated in response to an action of an object proximate to a proximity sensor of the computing device is detected. The proximity sensor signal corresponds to the security message. Use of the resource is authorized based on the proximity sensor signal.

[0006] According to further embodiments, a hand wave may be detected over the proximity sensor. A finger action on the device may also be detected near the proximity sensor.

[0007] According to some embodiments, the resource may correspond to a telephone call. The resource may correspond to a financial transaction. The resource may correspond to a text or email communication. Other resources may be considered.

[0008] According some embodiments, it is determined that a security check corresponds to a request for a resource on a computing device. A security message is provided for display on the computing device based on the security check. A non-contact sensor signal generated in response to an action of an object proximate to a non-contact sensor of the computing device is detected. The non-contact sensor signal corresponds to the security message. Use of the resource is authorized based on the non-contact sensor signal. The non-contact sensor may be a light sensor. The non-contact sensor may be a proximity sensor.

[0009] Some other embodiments are directed to related methods, systems and computer program products.

[0010] It is noted that aspects described with respect to one embodiment may be incorporated in different embodiments although not specifically described relative thereto. That is, all embodiments and/or features of any embodiments can be combined in any way and/or combination. Moreover, other systems, methods, and/or computer program products according to embodiments will be or become apparent to one with skill in the art upon review of the following drawings and detailed description. It is intended that all such additional systems, methods, and/or computer program products be included within this description, be within the scope of the present invention, and be protected by the accompanying claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] Embodiments of the present disclosure are illustrated by way of example and are not limited by the accompanying figures with like references indicating like elements.

[0012] FIG. 1 is a diagram of an action detected by a sensor of a computing device, according to various embodiments described herein;

[0013] FIG. 2 is a diagram of another action detected by a sensor of a computing device, according to various embodiments described herein;

[0014] FIG. 3 is a diagram of another action detected by a sensor of a computing device, according to various embodiments described herein;

[0015] FIG. 4 is a flow chart illustrating a process for performing a physical security check, according to various embodiments described herein;

[0016] FIG. 5 is a diagram of a system for performing a physical security check, according to various embodiments described herein; and

[0017] FIG. 6 is a block diagram of a computing device in which embodiments can be implemented.

DETAILED DESCRIPTION

[0018] Embodiments of the present disclosure will be described more fully hereinafter with reference to the accompanying drawings. Other embodiments may take many different forms and should not be construed as limited to the embodiments set forth herein. Like numbers refer to like elements throughout.

[0019] The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting to other embodiments. As used herein, the singular forms "a", "an" and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms "comprises," "comprising," "includes" and/or "including" when used herein, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

[0020] Unless otherwise defined, all terms (including technical and scientific terms) used herein have the same meaning as commonly understood by one of ordinary skill in the art to which this invention belongs. It will be further understood that terms used herein should be interpreted as having a meaning that is consistent with their meaning in the context of this specification and the relevant art and will not be interpreted in an idealized or overly formal sense unless expressly so defined herein.

[0021] As will be appreciated by one skilled in the art, aspects of the present disclosure may be illustrated and described herein in any of a number of patentable classes or context including any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof. Accordingly, aspects of the present disclosure may be implemented as entirely hardware, entirely software (including firmware, resident software, micro-code, etc.) or combined software and hardware implementation that may all generally be referred to herein as a "circuit," "module," "component," or "system." Furthermore, aspects of the present disclosure may take the form of a computer program product embodied in one or more computer readable media having computer readable program code embodied thereon.

[0022] Existing malware defenses for mobile devices may not be sufficient to detect sophisticated malware, without considering the special characteristics of mobile device malware. Mobile devices, such as smartphones, are personal devices. That is, the end user is a human being. Therefore, legitimate access to sensitive services such as premium calls, SMS or Near Field Communication (NFC) usually involves different types of human activity such as dialing a phone number, typing a message, or some type of physical gesture by the human user. Malware found on mobile devices attempts to access sensitive services without the user's awareness or involvement. Therefore, one way to detect such unauthorized, and potentially malicious, behavior is to validate whether an action is initiated by pure software or by a human user.

[0023] Certain services may be initiated by a user touching a keypad or touchscreen, which generates hardware interruptions for each touch event. A purely software generated activity (or malware generated activity), on the other hand, will not explicitly generate a hardware interrupt. Although a simple touch may be believed to be effective for malware detection, it may not be helpful to detect more sophisticated malware, such as pickpocket

malware. This is because the pickpocket malware is typically activated by a user playing a free game, such as tic-tac-toe, which already involves touch screen activity that can generate hardware interrupts. Some security applications may attempt to check whether there is just any user activity. However, some embodiments described herein may check whether there is a predefined user-aware activity. This may provide more fine-grained access control to detect even sophisticated malware.

[0024] According to various embodiments, lightweight malware detection mechanisms for mobile devices based on human gesture recognition are described. Some mechanisms may use sensors already available on current mobile devices with little or no additional user involvement. Certain explicit actions by a user may be detected using the proximity sensor of a mobile device.

[0025] One goal of a proximity sensor is to detect the presence or movement of a nearby object that is not necessarily in physical contact with the sensor or device. This sensor may work by sending an electromagnetic signal and analyzing the reflection or change in the electromagnetic field. The range of a proximity sensor may be small, such as a few centimeters. Different forms of proximity sensors may be used. Human gestures that use the proximity sensor do not interfere with other gestures made while interacting with the touch screen display, and significantly reduce the False Positive Rate (FPR).

[0026] According to some embodiments, a human gesture may trigger the proximity sensor in a way not likely to be exhibited in regular use of the device. For example, a gesture may fluctuate the readings of the proximity sensor quickly for a short duration of time. This could be easily detected by a user bringing in, and moving out, her hand or finger in close proximity to the sensor. Such gestures or actions may include, but are not limited to, a tap on the device near the proximity sensor. Figure 1 illustrates a tap gesture 100 near proximity sensor 104 of computing device 102, according to various embodiments.

The tap of a user finger may be on a touch screen 106 of computing device 102. Tap gesture 100 may be distinguished from a regular tap on touch screen 106 in the fact that it is near proximity sensor 104 while other taps may not be near proximity sensor 104. A tap, or any other action or gesture, is near or proximate to proximity sensor 104 if the action generates a proximity sensor signal useful for determining whether the gesture is likely a purposeful action. Proximity sensor 104 may be at a top center of a device, an upper corner of a device, offset from a center of the device, on a side of a device, on an edge of a device, on a lower center or corner of the device, or any other surface or location of a mobile device.

[0027] This gesture, or action, may correspond to an explicit request for the user to perform this gesture. The request may be made in a security message displayed on computing device 102. In some cases, identification of the proximity sensor may be necessary in educating the user. This can be done by a description or a simple arrow pointing to the proximity sensor.

[0028] According to some embodiments, another gesture may be a hand wave above the proximity sensor. A hand wave may be considered to include a wave of one or more fingers or other human extremities. Figure 2 illustrates hand wave gesture 200 over and/or proximate to proximity sensor 104, according to various embodiments.

[0029] According to some embodiments, another gesture may be a rub or slide of a finger on the device near the proximity sensor. Figure 3 shows a rub or slide of a finger on computing device 102 near proximity sensor 104, according to various embodiments. Again, this rub is not simply any rub or slide on the computing device. This rub is proximate to proximity sensor 104 such that proximity sensor 104 generates a signal useful for detection of a gesture, or explicitly requested gesture.

[0030] These proximity sensor gestures may be referred to as tap, wave or rub (TWR) proximity gestures for easier reference throughout this description. In some embodiments, any combination of these TWR proximity gestures may be requested and performed as part of a security check.

[0031] Algorithms used to detect quick fluctuations in proximity sensor readings may be simple and straightforward, which makes such embodiments lightweight. For example, when there is a proximity sensor reading change, the time duration of a gesture is recorded and the difference in time duration with a previous reading (perhaps 6 readings ago) is compared. If the difference is less than a predetermined time limit (e.g., with an upper bound of 1.5 seconds), the requested resource will be granted. Otherwise, the resource will remain unavailable, or the application will be halted or remain locked.

[0032] In some embodiments, a wave time limit may be set, such as 1500ms. An unlock time frame parameter may be set, such as 1000ms. Whenever the proximity sensor detects a change, it is recorded. Sensor readings may be indexed in an array. The array may be set to be only a certain number of readings. The array may operate to add a newest reading and drop an oldest reading. Time differences between a current reading any indexed previous reading may be determined. If a time difference is less than a wave time limit, the device may be unlocked for the duration of the unlock time frame parameter. The current reading index would then be increased by 1.

[0033] In further embodiments, proximity sensors may be programmed, trained or developed to detect variations in electromagnetic or other proximity detecting signals to differentiate between different user gestures over or near the proximity sensor.

[0034] These TWR proximity gestures are easy to use and have broad appeal. Whenever a sensitive service or resource is requested, a particular gesture needs to be detected (to

make sure it is a human generated activity) before the request can be granted. As gesture detection may be enforced every time a sensitive request is received, the described embodiment provides continuous monitoring of sensitive resources and services for protection from unauthorized access attempts by malware.

[0035] In some embodiments, TWR proximity gestures are detected based on proximity sensor data. In other embodiments, gestures such as TWR gestures may be detected using ambient light sensor readings. An advantage of a light sensor is that the hand would not need to be very close to the phone. This approach may utilize other signals, such as proximity and/or accelerometer data to reduce false positives, as simple phone movement may also trigger light values.

[0036] Figure 4 illustrates flowchart 400 with operations corresponding to a process for performing a security check, according to various embodiments of the disclosure. In block 402, it is determined that a security check corresponds to a request for a resource on a computing device. For example, an NFC financial transaction is to be made. The NFC applications or service coordinating with the NFC application may determine that a request for necessary resources requires a security check.

[0037] At block 404, a security message is provided for display on the computing device based on the security check. The message is a security message because the message is based on the security check. The security message may indicate that a specific user action must be performed to pass the security check. This action will be a gesture, not just another point of entry requiring a password, which can be spoofed. However, in some cases, some explicit, user-dependent physical gestures may act as physical passwords.

[0038] At block 406, a proximity sensor signal generated in response to an action of an object proximate to a proximity sensor of the computing device is detected. The proximity sensor signal corresponds to the security message. That is, the proximity sensor signal correlates with a signature of a gesture proximate to the proximity sensor requested by the security message. In some cases, this may be a simple robust gesture, such as a hand wave over the proximity sensor. In other cases, it may be a combination of gestures or a distinct gesture detectable by the proximity sensor. In some cases, a hand wave with all fingers may be distinguished from a hand wave of only one, two or three fingers.

[0039] At block 408, use of the resource is authorized based on the proximity sensor signal. The requested resource is made available. Continuing with the example of an NFC financial transaction, the transfer of money is completed. In some cases, this may mean resumption of a halted application, or allowance of the next step of a process.

[0040] According to some embodiments, the requesting and detecting of TWR proximity actions may be controlled from within the kernel-level middle layer between sensitive services and applications trying to access the services. In some embodiments, TWR proximity enhanced security may be enforced by a service on the mobile device. In other embodiments, such actions may be controlled from within an operating system and/or integrated specifically with the existing device permission model. A permission model, enhanced with TWR proximity security actions, provides continuous enforcement of access control to sensitive resources and services even after an application is installed on the platform.

[0041] Figure 5 shows a diagram 500 of a system 500 for performing a security check, according to some embodiments. Diagram 500 includes user 502, applications 504, TWR permission checker 510, sensor framework 520, middleware permission checker 530 and resources 540.

[0042] TWR permission checker 510 may add another layer of permission check before an existing platform middleware permission checker 530. If the malware is unable to maliciously alter the kernel control flow, a trusted path is formed with the operating system (OS). Intercepted permission requests may be handled by TWR permission checker 510.

[0043] TWR permission checker 510 stands in front of the original middleware permission check 520. When application 504 initiates a request to access a sensitive service, the request is intercepted by TWR permission checker 510. TWR permission checker 510 checks whether the requested service is protected by a certain gesture. If not, the request is forwarded to middleware permission checker 530 as usual. Otherwise, TWR permission checker 510 interacts with sensor framework 520 to request a security check. This may include collecting gesture data (e.g., tapping, rubbing, or waving proximity data). The captured data is then sent to TWR permission checker 510 for further process.

[0044] In some embodiments, gestures may be user-dependent or user-independent. A gesture is user-dependent if there is significant variation among gesture data from multiple participants for the same predefined gesture. A gesture is user-independent if either there is no apparent difference or the recognition process does not differentiate among user data from multiple participants. TWR proximity gestures may be user-independent as they infer user activity by checking whether an action occurs proximate to a proximity sensor. TWR proximity gestures may also be user-dependent based on additional instructions or training.

[0045] If a required gesture is detected, the request is forwarded to middleware permission checker 530. Otherwise, the request for service access is rejected.

[0046] Various embodiments may not require application level changes nor require resource monitors to be added for each resource.

[0047] Implicit permission may be granted by user intent acquired by a gesture. However, security applications may be more effective with explicit requests for user action. In some cases, detection may involve a training phase. A user may perform the target action, such as tapping or waving multiple times. Proximity and/or accelerometer data of the action may be recorded and processed to generate an action template. The template may serve as a reference for real-time user action comparisons. A match indicates a valid user gesture to grant access to a resource.

[0048] Successful recognition rates (or FNR) can be affected due to different phone orientations. This is because in a certain orientation, it might be possible for hand movements to accidentally trigger the proximity sensor. In some embodiments, the OS can disable certain orientations to prevent accidental unlocking from taking place. Due to the location of the proximity sensor (which may be near the ear piece), only one of the orientations may need to be disabled, while others can safely be permitted, without lowering the overall usability.

[0049] Another possibility to avoid such an accidental unlocking in our scheme is to infer the orientation of the device based on accelerometer data. If a “dangerous orientation” is detected, the access can be disabled by default. To further extend this approach, it is natural to consider other explicit gestures, or other ways to infer the gestures.

[0050] Embodiments described herein may be battery-friendly. The TWR proximity gestures described above are short (may last only a few seconds at most) and may only need to turn on the underlying sensors momentarily. For example, it may be that only when the user requests access to a particular resource is the sensor is turned on and the (explicit)

gesture detection algorithm is executed. Once the kernel captures the required gesture, the permission will be granted to the active application and the sensor will be turned off. If the kernel fails to capture the gesture within certain duration, the sensor will be turned off and the application will be denied to use the resource. In the case of NFC services or implicit gestures, a tapping detection algorithm may be executed only when the NFC reader detects a nearby tag.

[0051] TWR proximity gestures or other proximity gestures may be used to prevent malware from making phone (premium) calls, performing NFC transactions, sending short message service (SMS) messages, sending emails, turning on a microphone, turning on a location tracker, or any other application that would benefit from a security check by an actual human user. The TWR proximity gestures, such as the hand wave over the proximity sensor, are gestures for security that are robust and lightweight in implementation. In some embodiments, TWR proximity gestures and related devices may include additional features as discussed in Appendix A, which is incorporated herein in its entirety.

[0052] As will be appreciated by one skilled in the art, aspects of the disclosure may be embodied as a method, data processing system, and/or computer program product. Furthermore, embodiments may take the form of a computer program product on a tangible computer readable storage medium having computer program code embodied in the medium that can be executed by a computing device.

[0053] FIG. 6 is an example computer device 600 in which embodiments of the present disclosure, or portions thereof, may be implemented as computer-readable code. For example, the components of TWR permission checker 510 or any other components of diagrams 100-300 and 500 or method 400 may be implemented in one or more computer devices 600 using hardware, software implemented with hardware, firmware, tangible

computer-readable storage media having instructions stored thereon, or a combination thereof and may be implemented in one or more computer systems or other processing systems. Components and methods in FIGS. 1-5 may be embodied in any combination of hardware and software.

[0054] Computing device 600 may include one or more processors 602, one or more non-volatile storage mediums 604, one or more memory devices 606, a communication infrastructure 608, a display screen 610, a communication interface 612 and one or more sensors 616. Computing device 600 may also have networking or communication controllers, input devices (keyboard, a mouse, touch screen, etc.) and output devices (printer or display).

[0055] Processor(s) 602 are configured to execute computer program code from memory devices 604 or 606 to perform at least some of the operations and methods described herein, and may be any conventional or special purpose processor, including, but not limited to, digital signal processor (DSP), field programmable gate array (FPGA), application specific integrated circuit (ASIC), and multi-core processors.

[0056] GPU 614 is a specialized processor that executes instructions and programs, selected for complex graphics and mathematical operations, in parallel.

[0057] Non-volatile memory storage 604 may include one or more of a hard disk drive, flash memory, and like devices that may store computer program instructions and data on computer-readable media. One or more of non-volatile storage memory 604 may be a removable storage device.

[0058] Volatile memory storage 606 may include one or more volatile memory devices such as but not limited to, random access memory. Communication infrastructure 608 may

include one or more device interconnection buses such as Ethernet, Peripheral Component Interconnect (PCI), and the like.

[0059] Typically, computer instructions are executed using one or more processors 602 and can be stored in non-volatile memory storage 604 or volatile memory storage 606.

[0060] Display screen 610 allows results of the computer operations to be displayed to a user or an application developer.

[0061] Communication interface 612 allows software and data to be transferred between computer system 600 and external devices. Communication interface 612 may include a modem, a network interface (such as an Ethernet card), a communications port, a PCMCIA slot and card, or the like. Software and data transferred via communication interface 612 may be in the form of signals, which may be electronic, electromagnetic, optical, or other signals capable of being received by communication interface 612. These signals may be provided to communication interface 612 via a communications path. The communications path carries signals and may be implemented using wire or cable, fiber optics, a phone line, a cellular phone link, an RF link or other communications channels. According to an embodiment, a host operating system functionally interconnects any computing device or hardware platform with users and is responsible for the management and coordination of activities and the sharing of the computer resources.

[0062] Sensors 616 may include one or more sensors, including but not limited to, an accelerometer, proximity sensor, ambient light sensor, magnetometer, temperature sensor, pressure sensor, or any other sensors that may detect physical movement in relation to or contact with computing device 600.

[0063] Any combination of one or more computer readable media may be utilized. The computer readable media may be a computer readable signal medium or a computer readable storage medium. A computer readable storage medium may be, for example, but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing. More specific examples (a non-exhaustive list) of the computer readable storage medium would include the following: a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any suitable combination of the foregoing. In the context of this document, a computer readable storage medium may be any tangible medium that can contain, or store a program for use by or in connection with an instruction execution system, apparatus, or device.

[0064] A computer readable signal medium may include a propagated data signal with computer readable program code embodied therein, for example, in baseband or as part of a carrier wave. Such a propagated signal may take any of a variety of forms, including, but not limited to, electro-magnetic, optical, or any suitable combination thereof. A computer readable signal medium may be any computer readable medium that is not a computer readable storage medium and that can communicate, propagate, or transport a program for use by or in connection with an instruction execution system, apparatus, or device. Program code embodied on a computer readable signal medium may be transmitted using any appropriate medium, including but not limited to wireless, wireline, optical fiber cable, RF, etc., or any suitable combination of the foregoing.

[0065] Computer program code for carrying out operations for aspects of the present disclosure may be written in any combination of one or more programming languages,

including an object oriented programming language such as Java, JavaScript, Scala, Smalltalk, Eiffel, JADE, Emerald, C++, C#, VB.NET, Python or the like, conventional procedural programming languages, such as the "C" programming language, Visual Basic, Fortran 2003, Perl, COBOL 2002, PHP, ABAP, dynamic programming languages such as Python, Ruby and Groovy, or other programming languages. The program code may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider) or in a cloud computer environment or offered as a service such as a Software as a Service (SaaS).

[0066] Aspects of the present disclosure are described herein with reference to flowchart illustrations and/or block diagrams of methods, systems and computer program products according to embodiments. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create a mechanism for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

[0067] These computer program instructions may also be stored in a computer readable medium that when executed can direct a computer, other programmable data processing apparatus, or other devices to function in a particular manner, such that the instructions when stored in the computer readable medium produce an article of manufacture including instructions which when executed, cause a computer to implement the function/act specified in the flowchart and/or block diagram block or blocks. The computer program instructions may also be loaded onto a computer, other programmable instruction execution apparatus, or other devices to cause a series of operational steps to be performed on the computer, other programmable apparatuses or other devices to produce a computer implemented process such that the instructions which execute on the computer or other programmable apparatus provide processes for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

[0068] It is to be understood that the functions/acts noted in the blocks may occur out of the order noted in the operational illustrations. For example, two blocks shown in succession may in fact be executed substantially concurrently or the blocks may sometimes be executed in the reverse order, depending upon the functionality/acts involved. Although some of the diagrams include arrows on communication paths to show a primary direction of communication, it is to be understood that communication may occur in the opposite direction to the depicted arrows.

[0069] Many different embodiments have been disclosed herein, in connection with the above description and the drawings. It will be understood that it would be unduly repetitious and obfuscating to literally describe and illustrate every combination and subcombination of these embodiments. Accordingly, all embodiments can be combined in any way and/or combination, and the present specification, including the drawings, shall support claims to any such combination or subcombination.

[0070] The foregoing description of the specific embodiments will so fully reveal the general nature of the invention that others can, by applying knowledge within the skill of the art, readily modify and/or adapt for various applications such specific embodiments, without undue experimentation, without departing from the general concept of the present invention. Therefore, such adaptations and modifications are intended to be within the meaning and range of equivalents of the disclosed embodiments, based on the teaching and guidance presented herein.

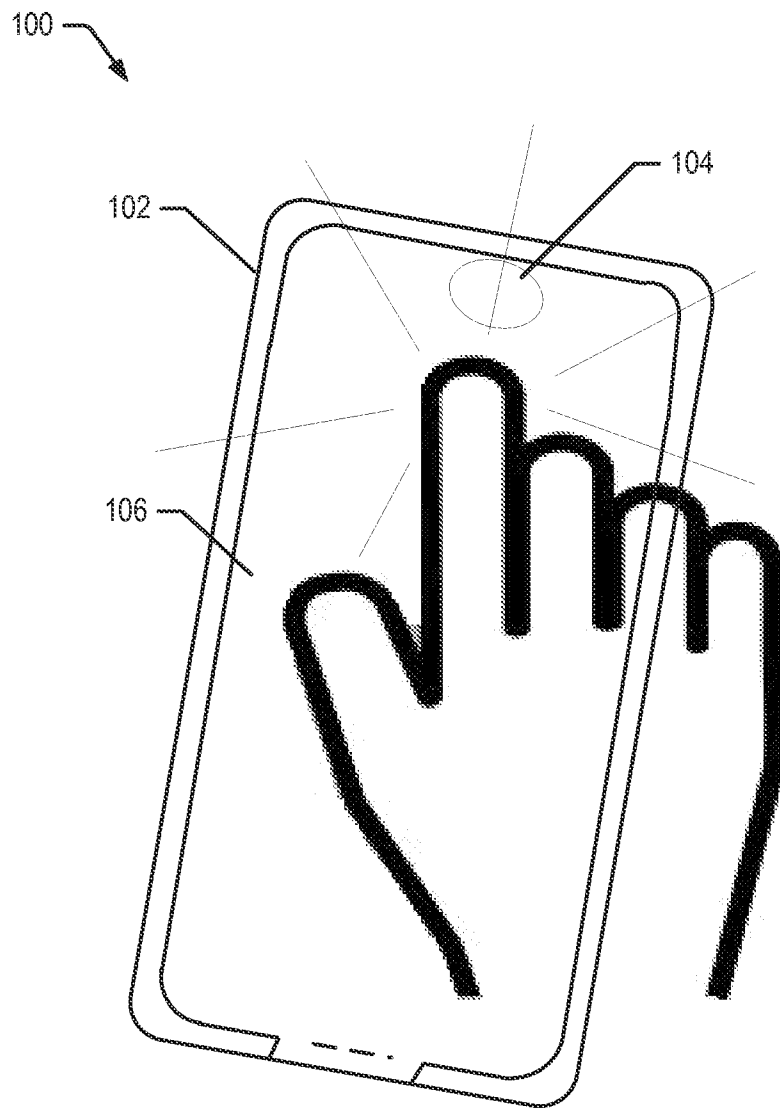
[0071] The breadth and scope of the present invention should not be limited by any of the above-described embodiments or any actual software code with the specialized control of hardware to implement such embodiments, but should be defined only in accordance with the following claims and their equivalents.

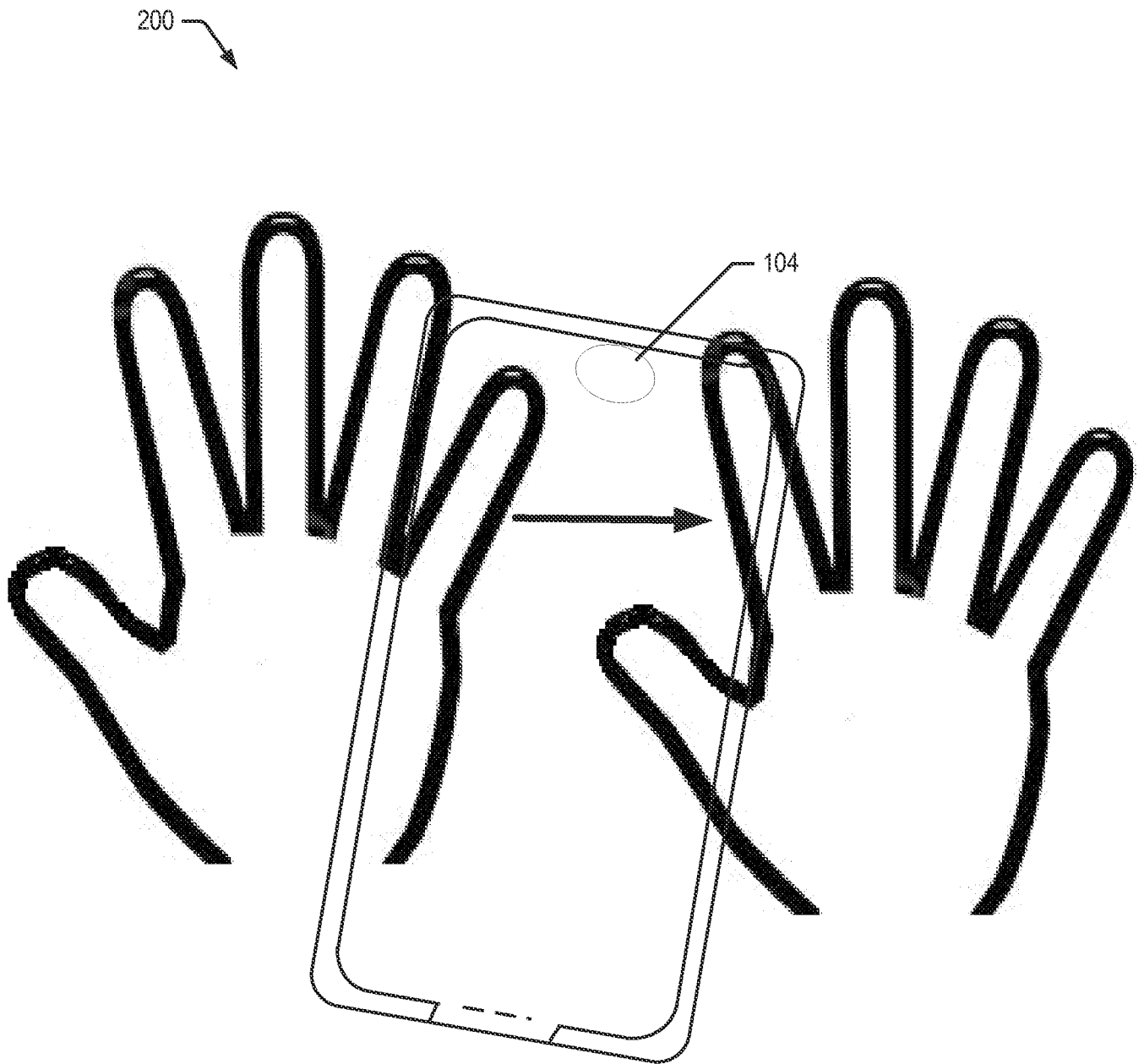
WHAT IS CLAIMED IS:

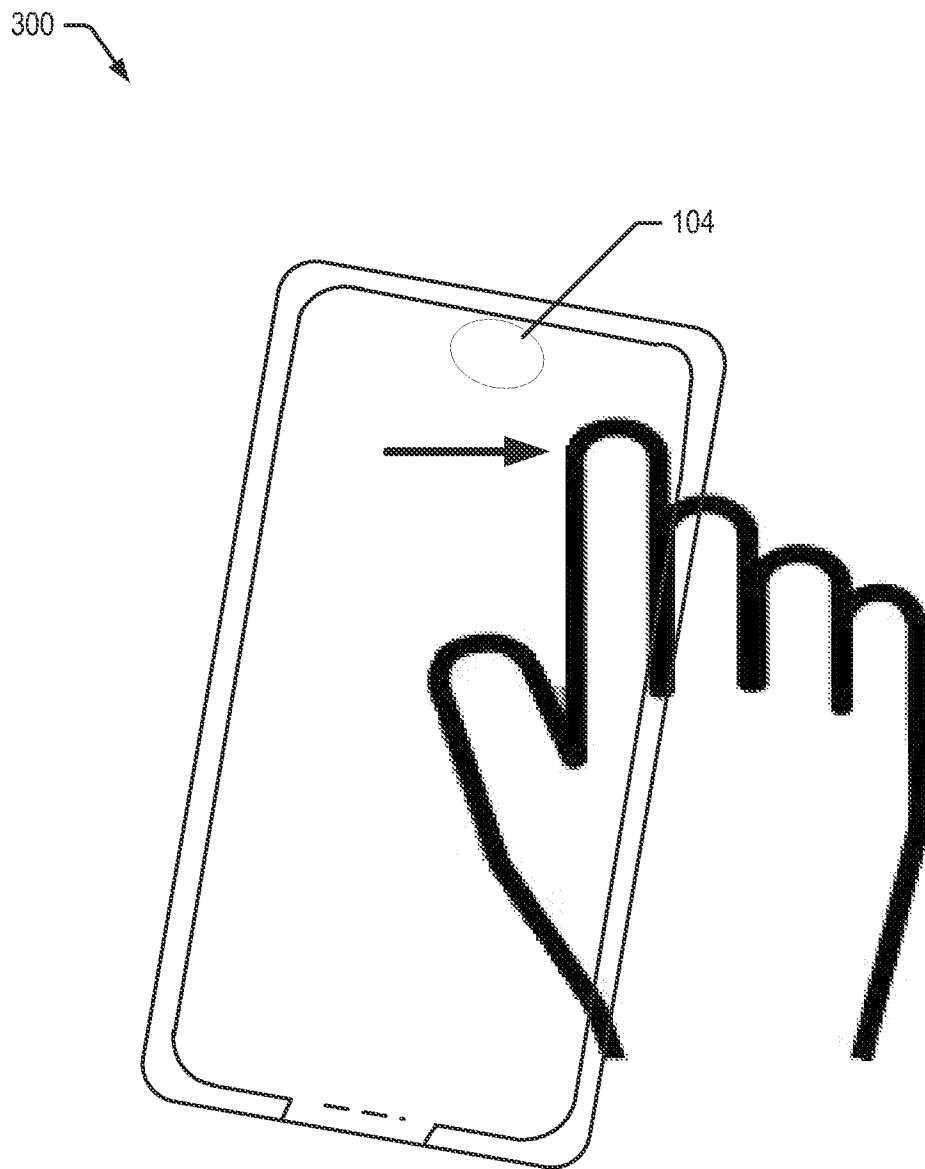
1. A computer-implemented method, comprising:
determining, by a computing device, that a security check corresponds to a request for a resource on the computing device;
providing a security message for display on the computing device based on the security check;
detecting a proximity sensor signal generated in response to an action of an object proximate to a proximity sensor of the computing device, wherein the proximity sensor signal corresponds to the security message; and
authorizing use of the resource based on the proximity sensor signal.
2. The method of claim 1, wherein the action of the object comprises a hand wave over the proximity sensor.
3. The method of claim 1, wherein the action of the object comprises a finger action near the proximity sensor.
4. The method of claim 1, wherein the resource corresponds to a telephone call.
5. The method of claim 1, wherein the resource corresponds to a financial transaction.
6. The method of claim 1, wherein the resource corresponds to a text or email communication.
7. The method of claim 1, further comprising:
detecting a second sensor signal generated in response to a second action, wherein the second sensor signal corresponds to the security message, and wherein the second sensor signal is different than the proximity sensor signal; and
authorizing use of the resource based on the proximity sensor signal and second sensor signal.

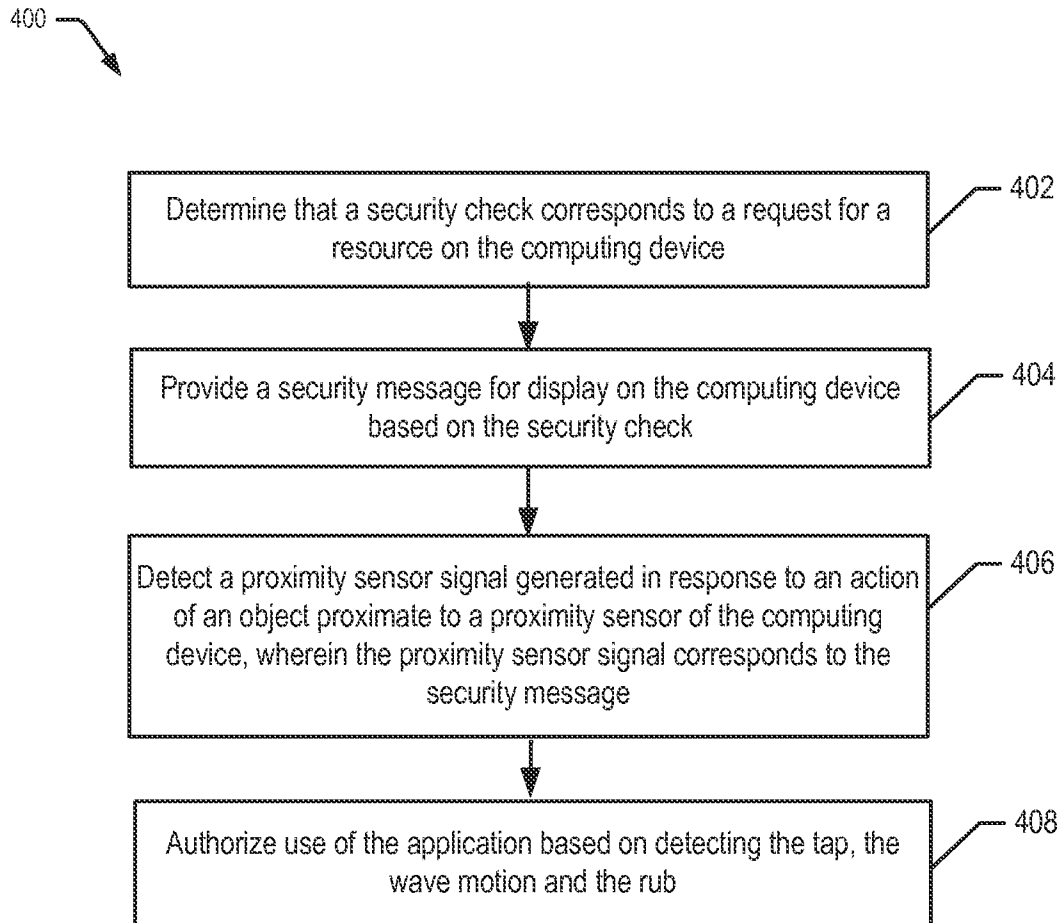
8. The method of claim 1, wherein the security message requests the action.
9. The method of claim 1, further comprising:
detecting a fluctuation in the proximity sensor signal within a predetermined time duration.
10. The method of claim 1, wherein the action of the object further comprises a tap on the computing device proximate the proximity sensor, a wave of an object over the proximity sensor and a rub on the computing device proximate the proximity sensor.
11. A computer-implemented method, comprising:
determining, by a computing device, that a security check corresponds to a request for a resource on the computing device;
providing a security message for display on the computing device based on the security check;
detecting a non-contact sensor signal generating by a non-contact sensor of the computing device in response to an action of an object proximate to a non-contact sensor, wherein the non-contact sensor signal corresponds to the security message;
and
authorizing use of the resource based on the non-contact sensor signal.
12. The method of claim 11, wherein the non-contact sensor is a light sensor.
13. The method of claim 11, wherein the non-contact sensor is a proximity sensor.
14. The method of claim 11, wherein the detecting comprises detecting a hand wave over the light sensor.
15. The method of claim 11, wherein the detecting comprises detecting a finger action near the proximity sensor.

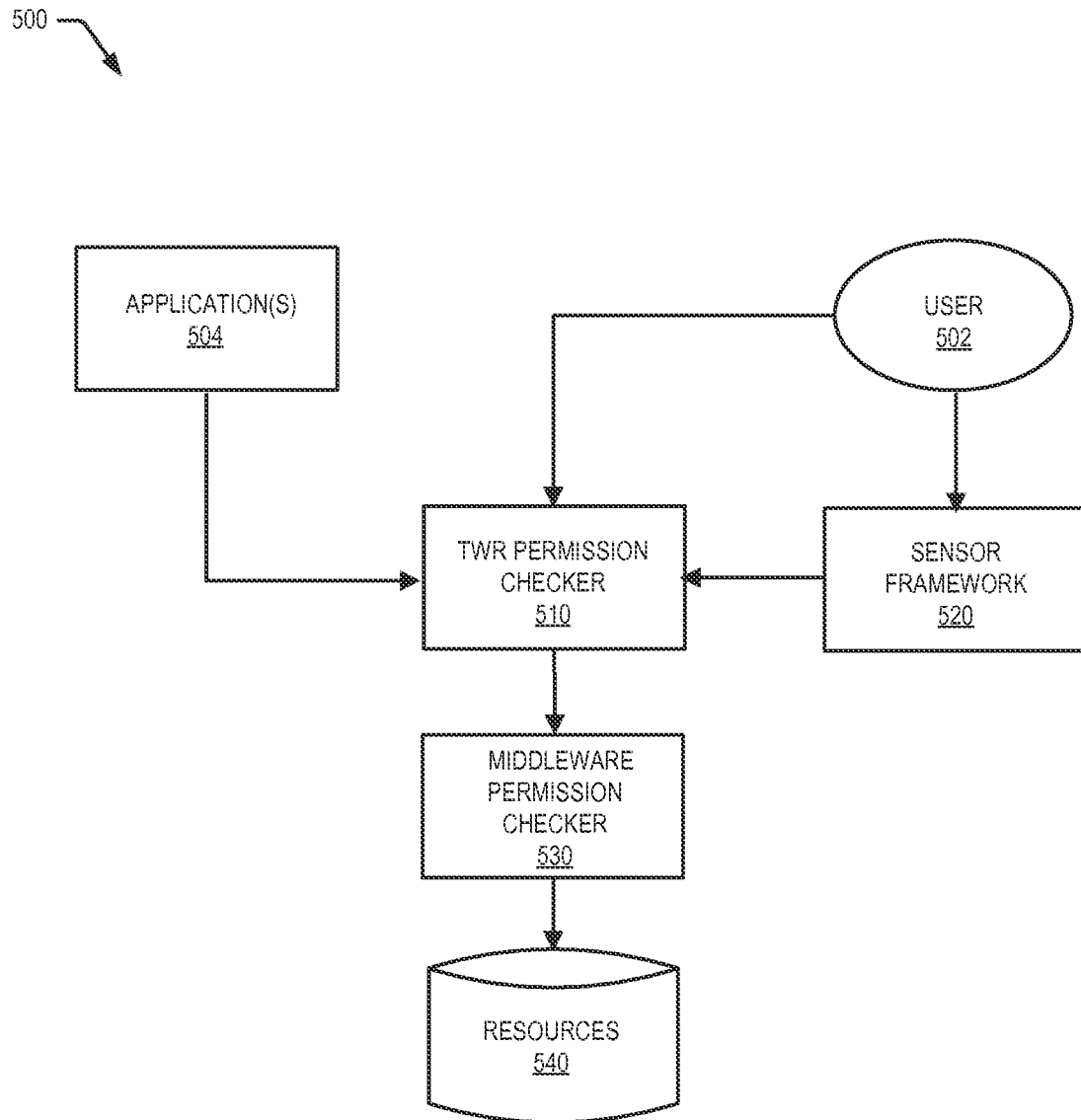
16. The method of claim 11, wherein the resource corresponds to a telephone call or financial transaction.
17. The method of claim 1, wherein detecting further comprises detecting a tap on the computing device proximate the light sensor, a wave of an object over the light sensor and a rub on the computing device proximate the light sensor.
18. A system, comprising:
a processor; and
a memory coupled to the processor and comprising computer readable program code embodied in the memory that when executed by the processor causes the processor to perform operations comprising:
determining, by a computing device, that a security check corresponds to a request for a resource on the computing device;
providing a security message for display on the computing device based on the security check;
detecting a proximity sensor signal generated in response to an action of an object proximate to a proximity sensor of the computing device, wherein the proximity sensor signal corresponds to the security message; and
authorizing use of the resource based on the proximity sensor signal.
19. The system of claim 18, the operations further comprising:
detecting a hand wave over the proximity sensor.
20. The system of claim 18, the operations further comprising:
detecting a finger action near the proximity sensor.

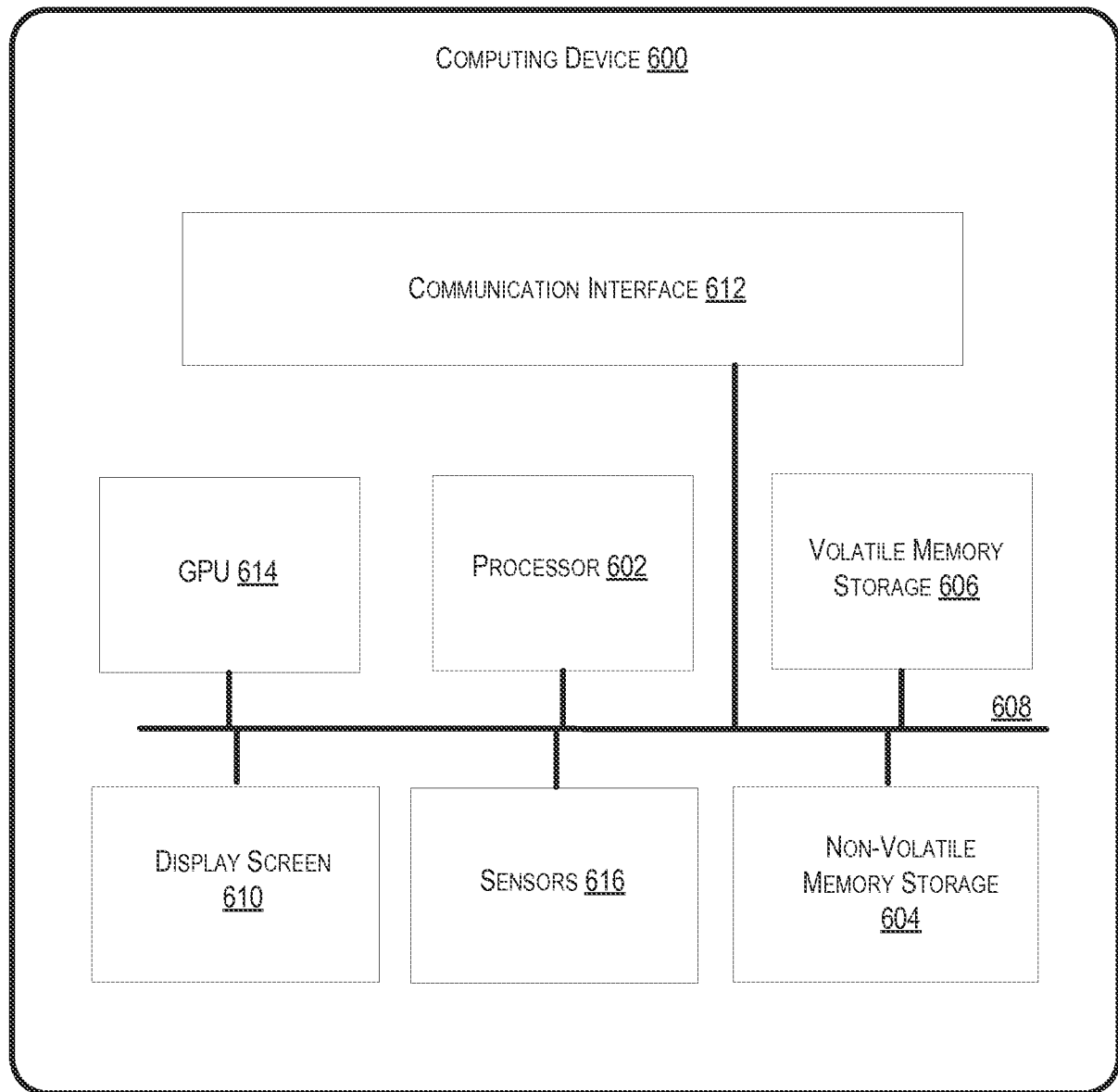
**FIGURE 1**

**FIGURE 2**

**FIGURE 3**

**FIGURE 4**

**FIGURE 5**

**FIGURE 6**

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/033495**A. CLASSIFICATION OF SUBJECT MATTER****G06F 21/00(2006.01)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 21/00; G06F 21/24; G06F 3/048; G06F 15/16; G06F 9/445; G06F 9/44; H04W 4/14; H04L 29/06

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: security check, message, resource, access, authorize, application, proximity sensor, light, non-contact, action

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2012-0317565 A1 (MICHAEL ANTHONY CARRARA et al.) 13 December 2012 See paragraphs [0016], [0021], [0038], [0044], [0051], [0107]; claims 1, 4; and figures 6A-7.	1-20
Y	US 2011-0312349 A1 (BABAK FORUTANPOUR et al.) 22 December 2011 See paragraphs [0014]-[0017], [0025]-[0027], [0030], [0033], [0043]-[0051], [0088]; claims 2, 39; and figures 1A, 2A, 6-8.	1-20
A	US 2011-0307831 A1 (CRISPIN COWAN et al.) 15 December 2011 See paragraphs [0050]-[0058]; and figure 5.	1-20
A	US 2012-0209923 A1 (GAURAV MATHUR et al.) 16 August 2012 See paragraphs [0010]-[0019], [0032]-[0035], [0050]; and figure 1.	1-20
A	US 8387141 B1 (IGOR ZHUKOV et al.) 26 February 2013 See column 1, line 46 - column 3, line 13; and figure 1.	1-20



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

21 August 2014 (21.08.2014)

Date of mailing of the international search report

21 August 2014 (21.08.2014)

Name and mailing address of the ISA/KR

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

Facsimile No. +82-42-472-7140

Authorized officer

AHN, Jeong Hwan

Telephone No. +82-42-481-8440



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2014/033495

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012-0317565 A1	13/12/2012	US 2014-109085 A1 US 8650550 B2	17/04/2014 11/02/2014
US 2011-0312349 A1	22/12/2011	WO 2011-159947 A1	22/12/2011
US 2011-0307831 A1	15/12/2011	None	
US 2012-0209923 A1	16/08/2012	WO 2012-109512 A1	16/08/2012
US 8387141 B1	26/02/2013	US 8732827 B1	20/05/2014