US 20060224882A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2006/0224882 A1

Chin (43) Pub. Date: Oct. 5, 2006

(54) METHOD AND SYSTEM FOR UNLOCKING A COMPUTING DEVICE

(75) Inventor: **Peter G. Chin**, Seattle, WA (US)

Correspondence Address:
MERCHANT & GOULD (MICROSOFT)
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903 (US)

(73) Assignee: **Microsoft Corporation**, Redmond, WA (US)

(21) Appl. No.: **11/095,677**

(22) Filed: **Mar. 31, 2005**

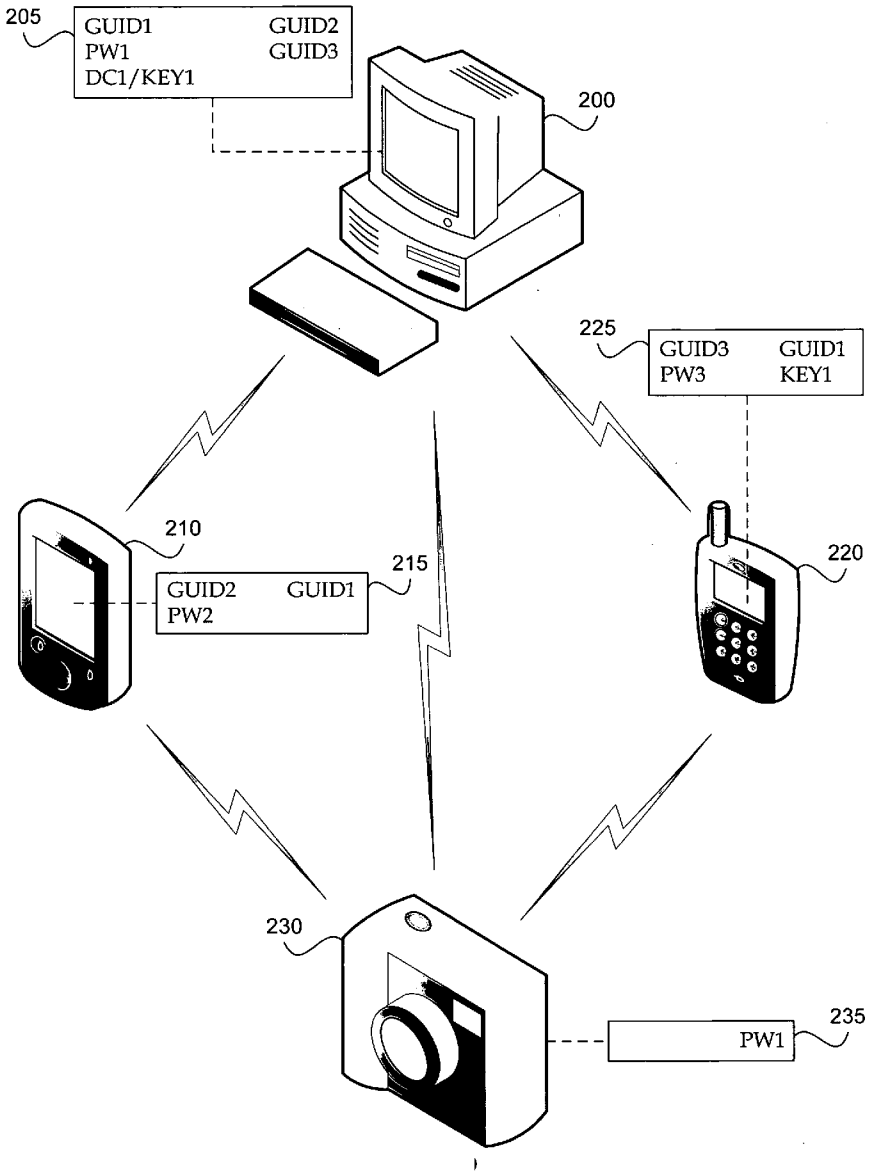
Publication Classification

(51) **Int. Cl.**
H04L 9/00 (2006.01)

(52) **U.S. Cl.** **713/150**

(57) **ABSTRACT**

A password locked computing device may be unlocked by coupling the locked device to a password unlocked computing device that is associated with the same user as the locked device. If the devices recognize each other as being associated with the same user, the locked computing device is automatically password unlocked without any password associated with the locked computing device being entered by the user.



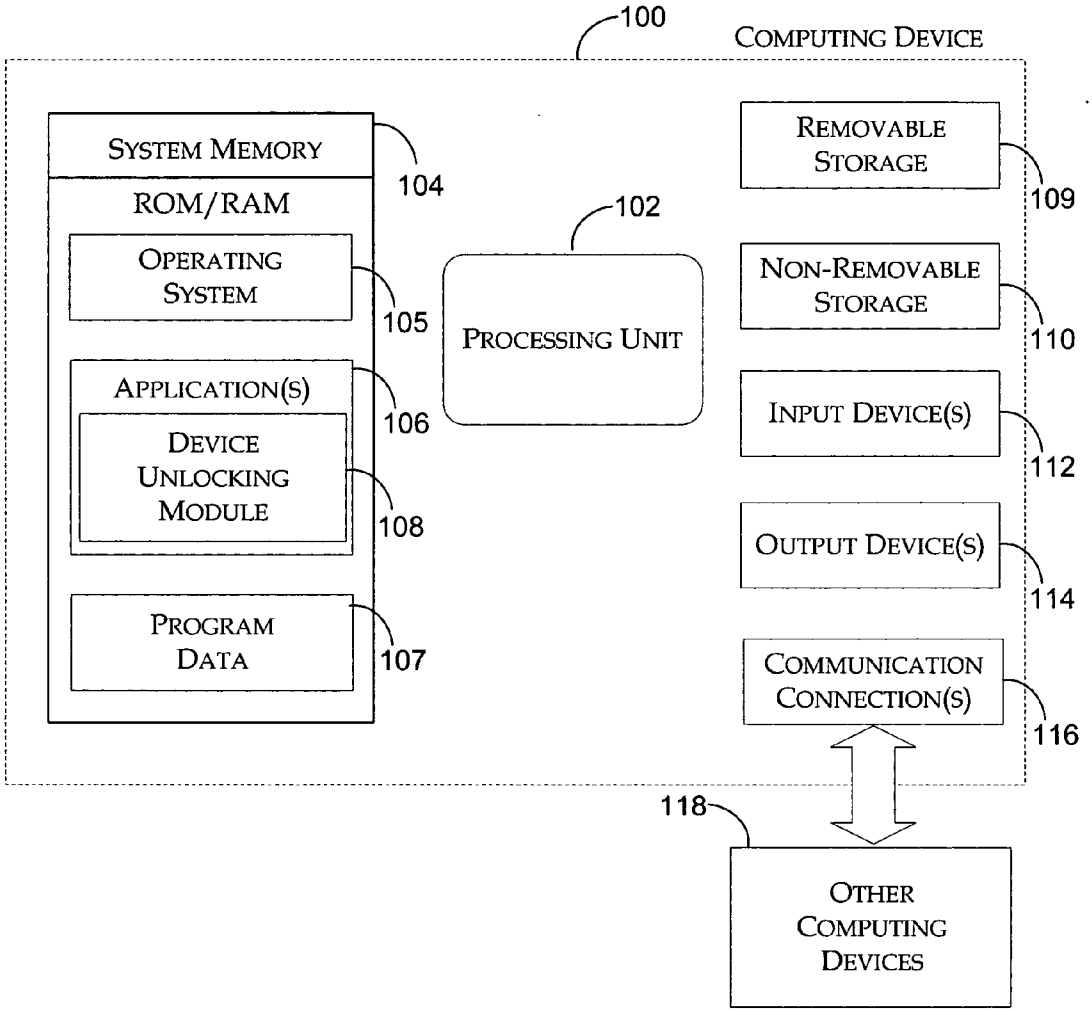


Fig. 1

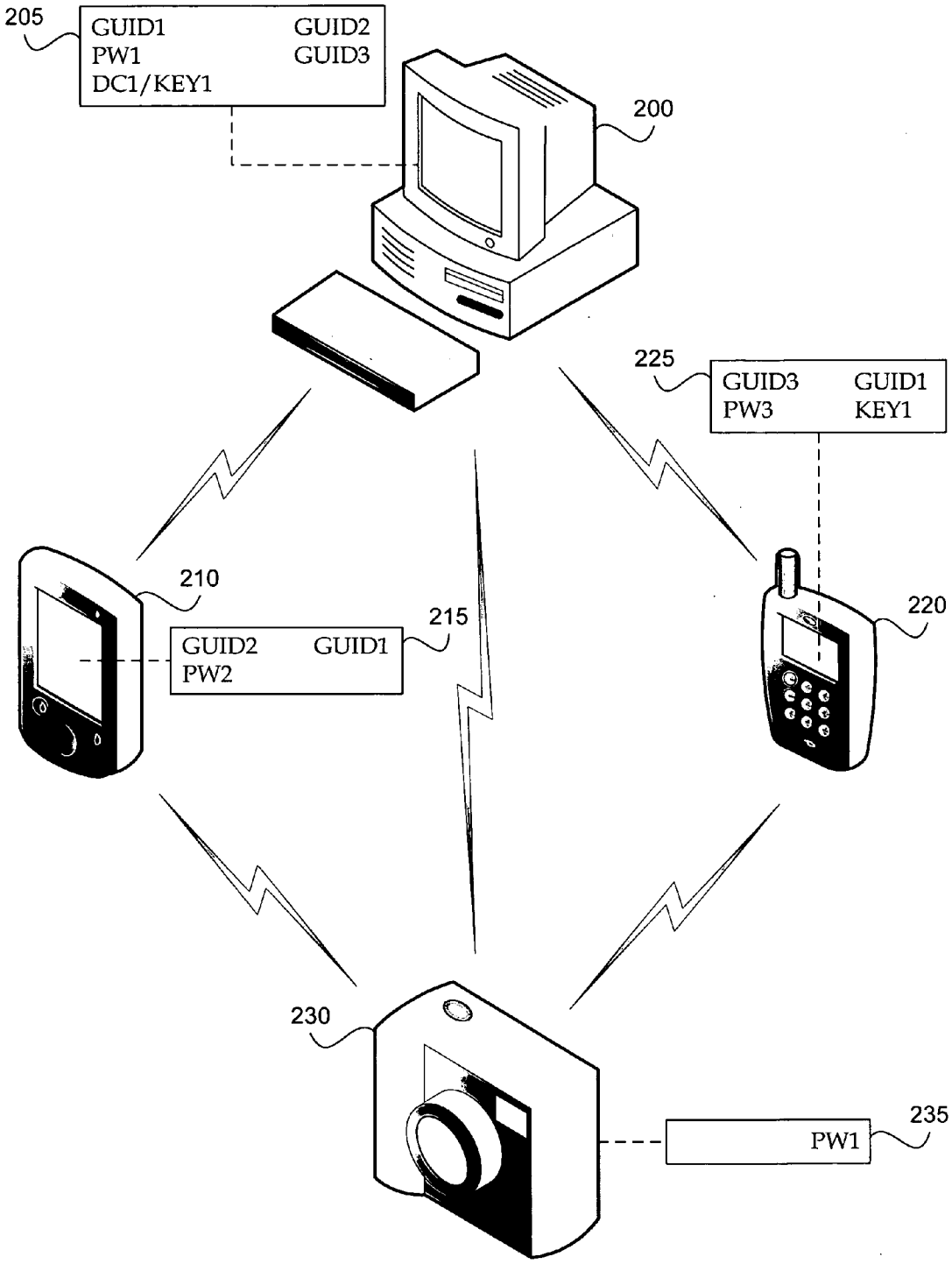


Fig. 2

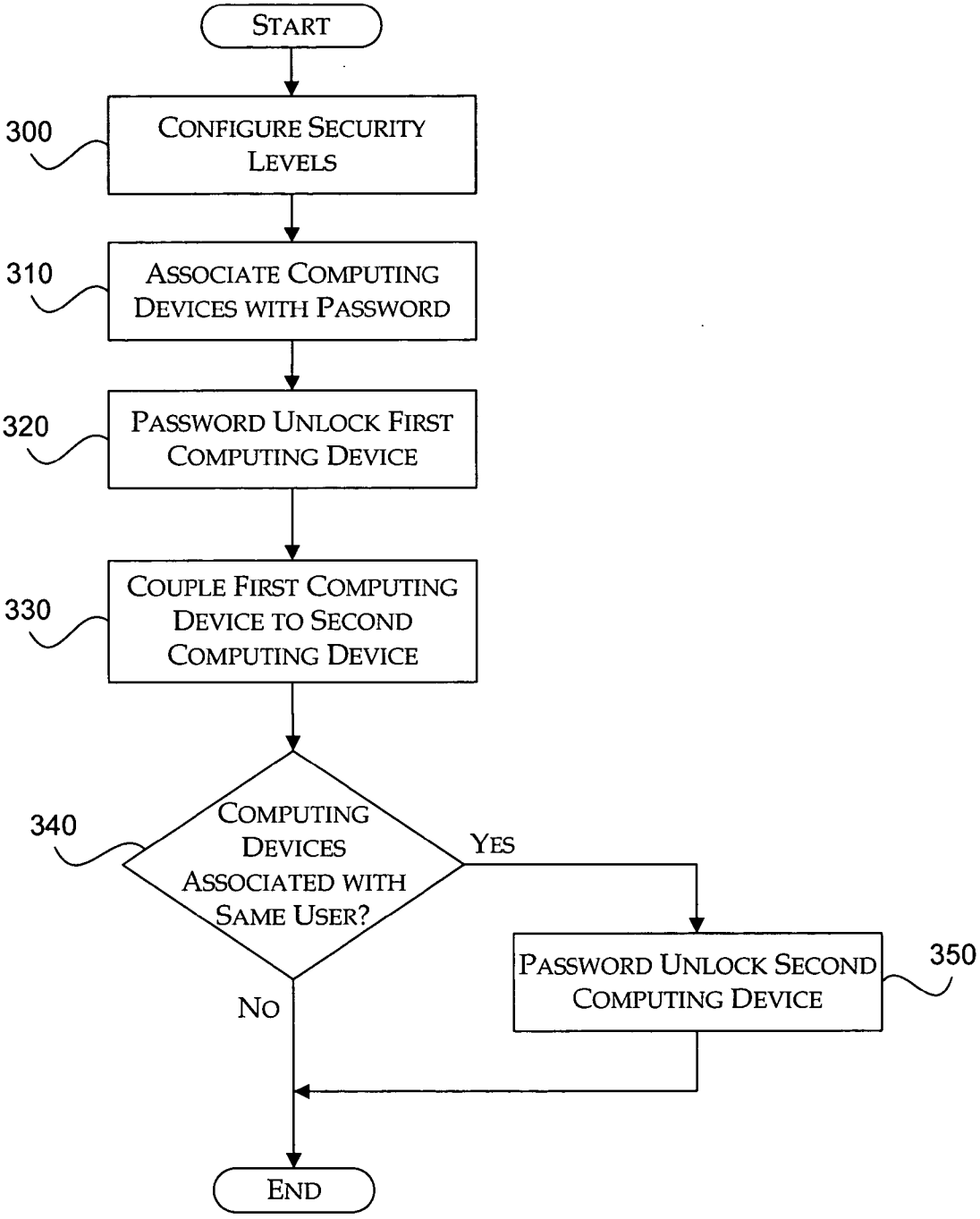


Fig. 3

METHOD AND SYSTEM FOR UNLOCKING A COMPUTING DEVICE

BACKGROUND

[0001] Digital security is major concern for many organizations. Computing devices are commonly password protected such that a device is locked when powered on to prevent unauthorized users from accessing information stored on the locked device. When synchronizing two computing devices both devices must be password unlocked before synchronization may be initiated. Some computing devices, such as personal digital assistants (PDAs), are designed for quick reference. However, the usefulness of the quick reference feature is diluted when a user is required to enter a password each time the PDA is accessed. Furthermore, many people commonly use different computing devices on a regular basis. Remembering a password for each device is burdensome for users, especially when organizations require passwords to be changed on a regular basis.

SUMMARY

[0002] The present disclosure is directed to a method and system for unlocking a computing device. A first computing device may be password unlocked by entering a password associated with the first computing device. A second computing device may be password locked. The second computing device may be associated with the same user as the first computing device. The first computing device couples to the second computing device. If the devices recognize each other as being associated with the same user, the second computing device is automatically password unlocked without any password associated with the second computing device being entered by the user. The computing devices may recognize each other as being associated with the same authorized user based on recognition information such as device identifiers, a key/certificate recognition partnership, or password verification.

[0003] In accordance with one aspect of the invention, a first computing device is coupled to a second computing device. The first computing device is password unlocked and the second computing device is password locked. A determination is made whether the first computing device and the second computing device recognize each other based on recognition information associated with the first computing device and the second computing device. The second computing device is unlocked when the first computing device and the second computing device recognize each other.

[0004] Other aspects of the invention include system and computer-readable media for performing these methods. The above summary of the present disclosure is not intended to describe every implementation of the present disclosure. The figures and the detailed description that follow more particularly exemplify these implementations.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] **FIG. 1** illustrates a computing device that may be used according to an example embodiment of the present invention.

[0006] **FIG. 2** illustrates functional block diagram of a

[0007] **FIG. 3** illustrates an operational flow diagram illustrating a process for unlocking a computing device, in accordance with at least one feature of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0008] The present disclosure is directed to a method and system for unlocking a computing device. A first computing device may be password unlocked by entering a password associated with the first computing device. A second computing device may be password locked. The first computing device couples to the second computing device. If the devices recognize each other as being associated with the same user, the second computing device is automatically password unlocked without any password associated with the second computing device being entered by the user.

[0009] Embodiments of the present invention now will be described more fully hereinafter with reference to the accompanying drawings, which form a part hereof, and which show, by way of illustration, specific exemplary embodiments for practicing the invention. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Among other things, the present invention may be embodied as methods or devices. Accordingly, the present invention may take the form of an entirely hardware embodiment, an entirely software embodiment or an embodiment combining software and hardware aspects. The following detailed description is, therefore, not to be taken in a limiting sense.

Illustrative Operating Environment

[0010] With reference to **FIG. 1**, one example system for implementing the invention includes a computing device, such as computing device **100**. Computing device **100** may be configured as a client, a server, a mobile device, or any other computing device that interacts with data in a network based collaboration system. In a very basic configuration, computing device **100** typically includes at least one processing unit **102** and system memory **104**. Depending on the exact configuration and type of computing device, system memory **104** may be volatile (such as RAM), non-volatile (such as ROM, flash memory, etc.) or some combination of the two. System memory **104** typically includes an operating system **105**, one or more applications **106**, and may include program data **107**. A device unlocking module **108**, which is described in detail below with reference to **FIGS. 2 and 3**, is implemented within applications **106**.

[0011] Computing device **100** may have additional features or functionality. For example, computing device **100** may also include additional data storage devices (removable and/or non-removable) such as, for example, magnetic disks, optical disks, or tape. Such additional storage is illustrated in **FIG. 1** by removable storage **109** and non-removable storage **110**. Computer storage media may include volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information, such as computer readable instructions, data structures, program modules, or other data.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.