EXHIBIT 2

(12) **United States Patent**
Schiffer

(10) **Patent No.: US 6,871,063 B1**
(45) **Date of Patent: Mar. 22, 2005**

(54) **METHOD AND APPARATUS FOR CONTROLLING ACCESS TO A COMPUTER SYSTEM**

(75) Inventor: **Jeffrey L. Schiffer**, Palo Alto, CA (US)

(73) Assignee: **Intel Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 319 days.

(21) Appl. No.: **09/607,804**

(22) Filed: **Jun. 30, 2000**

(51) **Int. Cl.**[7] **H04M 1/66**

(52) **U.S. Cl.** **455/410**; 455/419; 455/411; 455/424; 455/426.1; 455/269; 455/418; 455/420

(58) **Field of Search** 455/419, 411, 455/129, 269, 410, 418, 420

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,223,029 B1 * 4/2001 Stenman et al. 455/420

6,405,027 B1 * 6/2002 Bell 455/403

FOREIGN PATENT DOCUMENTS

WO WO 00/31608 * 6/2000

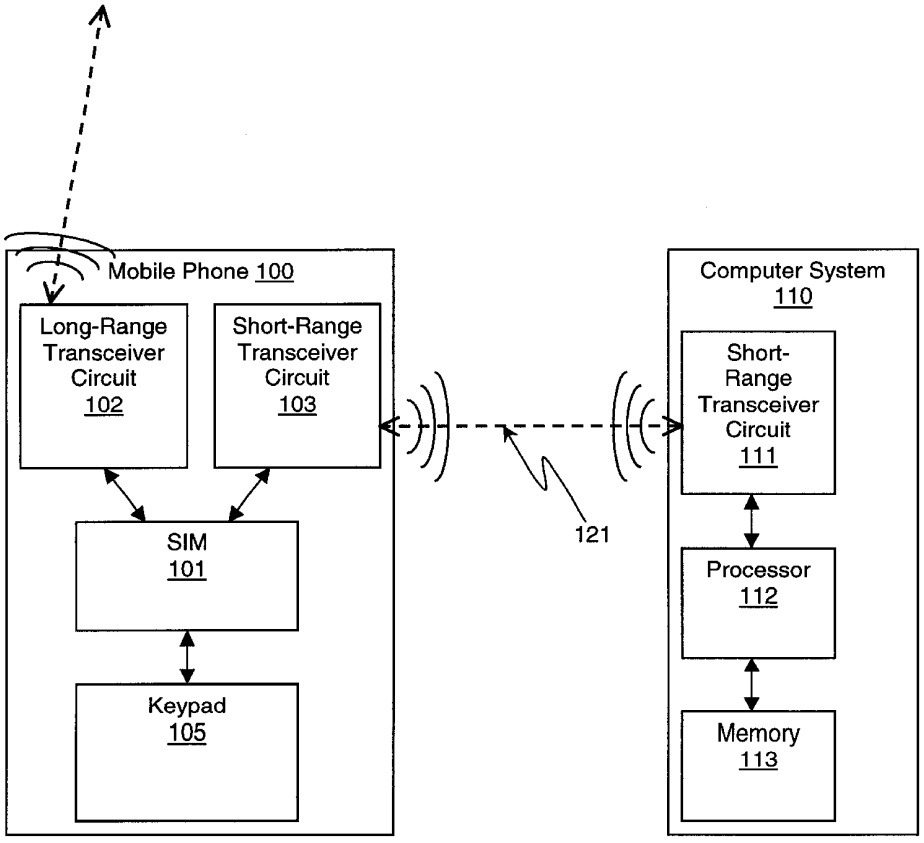
* cited by examiner

Primary Examiner—Erika Gary
Assistant Examiner—David Nguyen
(74) *Attorney, Agent, or Firm*—David N. Tran

(57) **ABSTRACT**

For one embodiment, a short-range, wireless communication link, such as a Bluetooth link, is established between a mobile phone and a computer system. The mobile phone transmits an access code via the link to the computer system. The access code is generated using data stored in the subscriber identity module (SIM) in the mobile phone. Access to the computer system is granted in response to receiving the access code. In this manner, the SIM is used not only to identify the user during cellular phone calls (or other long-range, wireless communication) but also to authenticate the user and to gain access to a computer system.

16 Claims, 2 Drawing Sheets



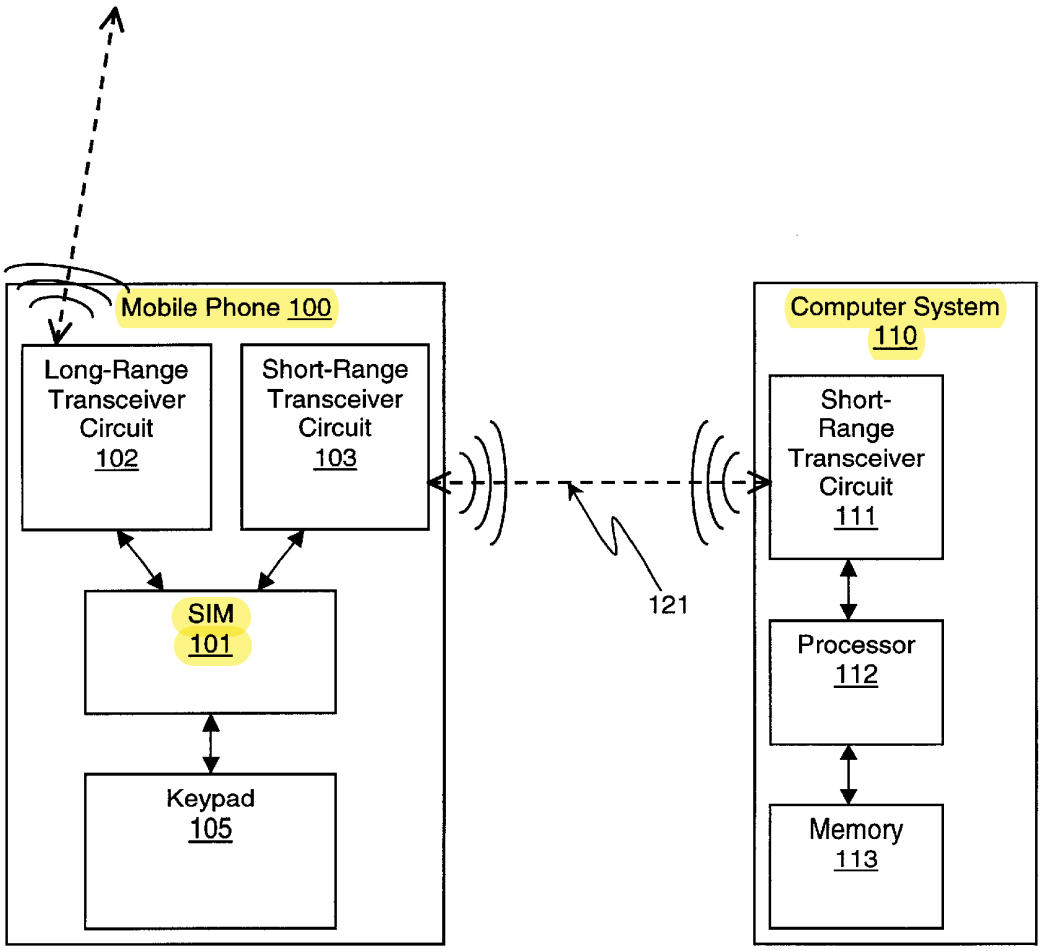


Figure 1

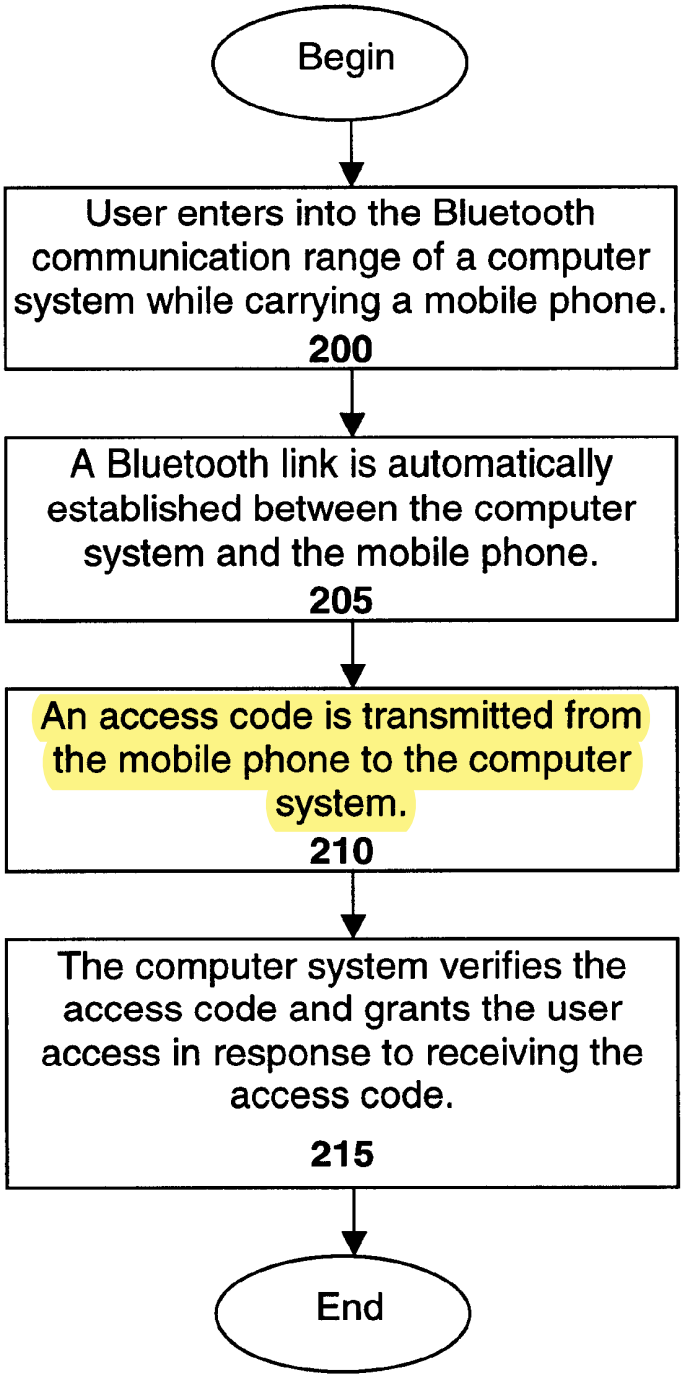


Figure 2

METHOD AND APPARATUS FOR CONTROLLING ACCESS TO A COMPUTER SYSTEM

The present invention relates to computer systems and more particularly to controlling access to a computer system by granting access to a user having a device that wirelessly transmits an access code.

BACKGROUND

Computer systems, from small handheld electronic devices to medium-sized mobile and desktop systems to large servers and workstations, are becoming increasingly pervasive in our society. As such, people are becoming more reliant on computer systems to store and access information, much of which may be confidential. To maintain the confidentiality of this information, some computer systems may be voluntarily "locked" or "secured" by a user. When a computer system is locked, access to the computer system may be limited. This not only serves to maintain the confidentiality of information stored on the computer system but also deters theft of the computer system.

One way in which access to a computer system may be limited is by password-protecting the system. In a password-protected computer system, access to the system is only granted to a user that enters a proper password. One advantage to this type of protection mechanism is that the user need not carry special security devices, such as keys or cards, to gain access to the computer system. The user need only remember a password. Another advantage to this type of protection is that different levels of access may be granted according to the password entered.

Unfortunately, password-protected computer systems may not be secure. There are a number of ways to crack a password-protected computer system. For example, a thief or spy may surreptitiously observe a user when the user enters their password. Later, the thief may simply steal the computer system, confident in the knowledge that the system can be unlocked by the thief by entering the observed password. This security problem is particularly of concern to mobile computer users. Alternatively, the spy may log onto the computer system in the user's absence using the observed password. The spy may then access confidential information without the user knowing that their security has ever been compromised.

The present invention addresses this and other problems associated with the prior art.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example and not limitation in the accompanying figures in which like references indicate similar elements and in which:

FIG. **1** is a system formed in accordance with an embodiment of the present invention; and

FIG. **2** is a flow chart showing a method of the present invention;

DETAILED DESCRIPTION

In accordance with an embodiment of the present invention, the subscriber identity module (SIM) in a user's mobile phone is used to gain access to a locked computer system. Initially, access to the computer system is limited. When a user with a mobile phone comes into short-range, wireless communication range of the computer system, a short-range, wireless communication link is automatically established (i.e. established without user intervention). This short-range, wireless communication link may be a Bluetooth* link. (*Trademarks and trade names are the property of their respective owners.)

For one embodiment, the computer system transmits information to the mobile phone via the wireless link to indicate that access to the computer system is limited. In response, the mobile phone transmits an access code back to the computer system via the link. This access code is generated using data stored in the SIM in the mobile phone. After the computer system verifies the access code, access to the computer system is granted in response to receiving the access code.

In this manner, the SIM is used not only to identify the user during cellular phone calls (or other long-range, wireless communication) but also to authenticate the user to the computer system. Note that for one embodiment, the user may authenticate himself or herself to the mobile phone by, for example, entering a password into the mobile phone.

A more detailed description of embodiments of the present invention, including various configurations and implementations, is provided below.

FIG. **1** is a system formed in accordance with an embodiment of the present invention. Mobile phone **100** includes long-range transceiver circuit **102** along with short-range transceiver circuit **103**, both coupled to SIM **101**. Keypad **105** is also coupled to SIM **101**. Computer system **110** includes short-range transceiver circuit **111**, coupled to processor **112**, which is coupled to memory **113**.

Mobile phone **100** of FIG. **1** may be any mobile phone capable of long-range communication. For example, for one embodiment, mobile phone **100** is a cellular phone, in which case long-range transceiver circuit **102** may communicate with a cell base. For another embodiment, mobile phone **100** is a satellite phone, in which case long-range transceiver circuit **102** may communicate with a satellite or relay station.

SIM **101** of FIG. **1** includes a protected memory region having data stored therein. A protected memory region is a memory region that is not generally modifiable by typical users. Thus, important information may be securely stored in the protected memory region of SIM **101** with a low risk of being compromised. The data stored in the protected memory region of SIM **101** includes the subscriber identity number associated with the user of mobile phone **100**. This subscriber identity number may be securely programmed into SIM **101** by the manufacturer or distributor of mobile phone **100**.

The subscriber identity number may be unique to each mobile phone or mobile phone account holder. This number is used to uniquely identify the mobile phone subscriber when a mobile phone call (e.g. a cellular phone call) is placed via long-range transceiver circuit **102** of FIG. **1**. The subscriber identity number is wirelessly communicated, along with the user's voice/data communication, via long-range transceiver circuit **102**. The phone company then uses this subscriber identity number to bill the proper account holder.

As described in more detail below, in accordance with an embodiment of the present invention, data stored in the protected memory region of SIM **101** of FIG. **1**, including the subscriber identity number, is used to wirelessly authenticate the user to computer system **110** by transmitting an access code. Once the access code is verified, authentication is complete, and computer system **110** grants access to the user. Thus, the data in SIM **101** that is already used by the

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.