(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 April 2001 (26.04.2001)

PCT

(10) International Publication Number
WO 01/29731 A1

(51) International Patent Classification⁷: G06F 17/60

(21) International Application Number: PCT/US00/28387

(22) International Filing Date: 13 October 2000 (13.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/422,621 21 October 1999 (21.10.1999) US

(71) Applicant: **3COM CORPORATION** [US/US]; 5400 Bayfront Plaza, Santa Clara, CA 95052-8145 (US).

(72) Inventors: **THOMPSON, Curtis, Duane**; 1481 West Bluemont Drive, Taylorsville, UT 84123-6666 (US). **CROFT, Kenneth, A.**; 2159 South Hannibal Street, Salt Lake City, UT 84106 (US).

(74) Agents: **MASCHOFF, Eric, L.** et al.; Workman, Nydegger & Seeley, 1000 Eagle Gate Tower, 60 East South Temple, Salt Lake City, UT 84111 (US).

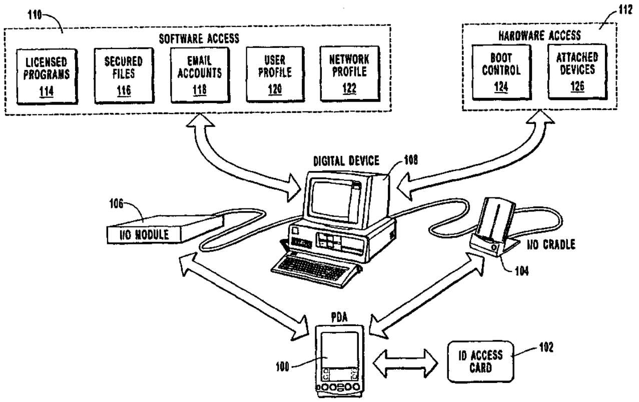
(81) Designated States *(national)*: CN, DE, FI, GB, JP, SE.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ACCESS CONTROL USING A PERSONAL DIGITAL ASSISTANT-TYPE



(57) Abstract: An access control system combining PDA functionality with user authentication so that only the authorized user or users may obtain access control codes from a PDA device for an access control point. The access control point can be a computer terminal (108), a computer file, a door, a checkstand, a visa authorization point, a gate, or other situation wherein high security is desirable. In a preferred embodiment, the access control system attaches to a computer (108) via a PDA cradle (104) and transmits access control codes that include a series of authentication codes or identification codes having encoded data stored within a PDA database. In another form of the invention, user authentication is obtained by comparing biometric data such as a fingerprint with digitally stored data of the authorized user. A decision to grant access affects the release, an electronic release or electronic strike, or electronic software hold. If desired, a write feature can be included into the system whereby each access control point accessed or attempted to be accessed by a PDA user will be recorded on the PDA to determine where access has been attempted. Additional records could be maintained along with the authentication I.D. including checking account information, credit card information,

ACCESS CONTROL USING A PERSONAL DIGITAL ASSISTANT-TYPE

BACKGROUND OF THE INVENTION

1. The Field of the Invention

This invention relates to a method for authorizing access control using a PDA device. More particularly, the invention relates to an access control system that uses a PDA device to reference secured data, which thereby facilitates implementation of a selective access policy by a service controller in communication with the PDA device.

2. Description of the Prior Art

One of the challenges of the modern consumer is to maintain a respectable size of their wallet without discarding any required information. As such an individual may be required to carry with their planner, a drivers license, a plurality of credit cards and gas cards, social security numbers, photographs of the family, personal identification, checkbooks, check ledgers, bank account numbers, a telephone list of frequent contacts, various business cards, business notes and other necessities. The net result is a wallet that no longer fits within the constraints of the user's purse or pocket.

Personal Digital Assistant (PDA) devices, like the 3Com PalmPilot®, provide a user with an easy, compact device that can hold all of a user's daily essentials in one place. A PDA device provides a user with quick and easy access to multiple applications customized to meet the individual user's needs. A successful PDA device is lightweight enough to carry everywhere and small enough to fit into a pocket, as a user won't use the PDA device if they don't carry it. Other desirable features found on a PDA device include instant information access, intuitive construction for easy use, conservative energy cell consumption, extensive personal calendaring features, a customized address book, a digital memo pad, an expense calculator, desktop e-mail connectivity, Internet compatibility, and local or remote database synchronization. While the development of PDA devices has dramatically reduced digital complexity for the user, holding thousands of addresses and hundreds of notes or e-mail messages in one portable device, PDA devices have not provided improved access control for the user. Security features in modern PDA devices focus on the data security, data backup, or access security to the specific PDA device. What is needed is a PDA device that provides access control codes to multiple security outlets or service controllers, including access to: desktop computers for boot up, selective computer data or programs, mechanical hardware such as electronic doors, and service identification numbers such as credit card numbers and checking

The development of new digital device features are driven by the need for the digital device to perform a specific function. As a result, access control issues are virtually a non-existent factor in the overall design of a digital device. Traditionally, physical security may have been present, but the single user nature of early digital devices did not require exhaustive security methods within the digital device itself. While PDA devices continue to operate in predominately single user environments, other digital devices require more emphasis on access control. With the development of multiple user operating systems, segregated work groups containing multiple users, and personalized desktops varying each computer display from one user to the next; access control is a desirable quality for a computer system.

Examples of computer data felt to require access control include secure files, personalized e-mail accounts, specific user profiles, specific network profiles, and access to licensed programs. A secure file may be created by a user encrypting the file with a password. E-mail accounts obtain limited security by archiving data into personalized data structures or by password protecting e-mail access. Access to specific user profiles and network profiles are often controlled by operating system passwords. Many licensed programs require that only a specific quantity of users within a company be granted access and that additional users are not allowed access to these program. This regulation is generally accomplished by either assigning an access control code to each authorized user or the licensed program may regulate a hard quantity limitation on the total number of copies of the program that can be running from a server at any one time. By focusing on access control mechanisms surrounding the files, productivity and efficiency are reduced. These problems are enhanced if an individual user regularly switches work station locations to different access points within the company. Hence, a portable system which provides all file, user, network, or licensing authentication for a particular user would be useful for a corporation in managing its computer usage or license usages and would increase the efficiency and productivity of the user. Not to mention the added benefit of no longer needing to remember all the passwords used for each "secure" application.

A variety of access control systems and devices presently exist, however; these access control systems do not interface or coordinate with PDA devices. Specifically, a user attempting to gain access to various resources within a company is often required to carry an access card, an access key, or an I.D. access badge. The user may be required to know an access number, a PIN number, a combination, a password, or to provide a computer authorization number. In addition to these standard electronic and mechanical biometric information such as fingerprint verification or a retinal scan. A system that provides all of the necessary access control information using a PDA device as a substitute for the aforementioned keys, cards, or passwords would considerably lessen the security delays and inefficiencies created by the multiple verification devices presently required to obtain site access authorization, not to mention the additional benefit of drastically reducing the extent and magnitude of security access devices necessary for any one individual to carry with them.

Another area presently mired by the excessive numbers associated with access control are commercial transactions for goods or services. Unless a participant is using cash, the service provider or supplier will likely be required to obtain a purchase order number, a credit card, or a check. To complete the transaction, additional physical identification may be required in the form of a drivers license, a passport, a purchase order, a check verification card, or a credit card authorization number. Once again, a system that could maintain these access controls within the parameters of a PDA device would be a marked improvement over the present state of the art.

SUMMARY AND OBJECTS OF THE INVENTION

The foregoing problems in the prior state of the art have been successfully overcome by the present invention which is directed to a system and method for coordinating the production of access control codes by a PDA device to multiple security outlets or service controllers. The system and method of the present invention is scalable in that the PDA device can be adapted to accommodate an unlimited variety of access control codes for a variety of electronic, mechanical, or electrical controllers. Furthermore, the invention allows for the attachment of identification access cards either to program the PDA device to produce the access control codes, to work in conjunction with the PDA device, or to function independent of but attached to the PDA device.

The system and method of the present invention utilize a PDA device to provide improved access control for a user. According to the present invention, a PDA device is programmed to provide various access control codes to multiple security outlets or service controllers, specifically including access codes for: desktop computers during the boot up process, selective secured computer data files, protected or licensed programs, mechanical hardware such as those used with electronic latch doors, and service identification numbers such as credit card numbers and checking accounts.

The present invention supports an access control process that may be summarized as follows. A user enters access control information into a database in order to allow a outlets. The user may also enter the access control information directly to the PDA device through an interface device. The access control information includes access control codes used to enable the boot-up process for a connected digital device. These codes may also be used to authorize the transfer of funds in a commercial transaction. Access control codes can instruct the PDA device to produce the enabling or disabling signal for an electronic lock on items as diverse as a door and a secured computer file. Just as there are many different types of access control codes, there are multiple methods of delivering the codes to a service controller or security outlet. One method is through the I/O cradle attached to the PDA device and the digital device. I/O cradles are usually attached to either the serial RS-232 port or the parallel port. Another interface method is between a PDA Infra-Red (IR) port and an I/O module attached to the digital device with a IR interface. A preferred embodiment of the present invention utilizes wireless transceiver, built into the PDA device to communicate with a receiver. Finally traditional interface parts, coils, or transmissions may be effectively used. These interfaces include RF, Wegand, magnetic, USB, or laser communication. A final potential embodiment includes integrating an IC chip into the digital device providing access control codes faster.

In one embodiment, the system and method of the present invention provides all the file, user, network, or licensing authentication necessary for a particular user. Once the PDA device is plugged into an I/O cradle, all of the necessary password verification or authentication is supplied by the PDA device. A less memory intensive approach calls for the storage of a solitary password within the PDA access control database which downloads a user profile from a network location. Additional security checks could be implemented to verify that the PDA device holder is the actual user without negatively affecting the efficiency and productivity of the user because of the overall reduction in the number of access control codes. Another embodiment maintains communication between the PDA device and the digital device through an I/O module, such as a wireless transceiver or IR port. If a wireless transceiver is used, the PDA device can download information from the user's workstation at any time or from any location. The wireless PDA device embodiment could alert a user when someone is attempting unauthorized access to the user's computer. Another embodiment utilizes the PDA device to provide the access control codes for a user and then retrieves a customized user desktop setting for the user specified by the PDA device. This feature allows an individual user to attach to any computer within a company's network and obtain their customized desktop. This feature allows for incredible flexibility and versatility, not to mention the added benefit

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.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE