

Inventor: BURKE, Christopher John
 Title: REMOTE ENTRY SYSTEM

POWER OF ATTORNEY

The specification of the above-identified patent application:

- is attached hereto
 was filed on **February 13, 2006** as U.S. Application Serial No. **10/568,207**.

I hereby revoke all previously granted powers of attorney in the above-identified patent application and appoint the following attorneys to prosecute said patent application and to transact all business in the Patent and Trademark Office connected therewith:

Michael E. Milz (Reg. No. 34,880)
 Robert D. Summers, Jr. (Reg. No. 57,844)

Please address all correspondence and telephone calls to Michael E. Milz in care of:

Brinks Hofer Gilson & Lionc
 P.O. Box 10395
 Chicago, Illinois 60610
 (312)321-4200

The undersigned hereby authorizes the U.S. attorneys named herein to accept and follow instructions from Martin Friedgut as to any action to be taken in the Patent and Trademark Office regarding this application without direct communication between the U.S. attorney and the undersigned. In the event of a change in the persons from whom instructions may be taken, the U.S. attorneys named herein will be so notified by the undersigned.

As required by 37 CFR 3.73(b)(1) and shown below, the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

Securicom (NSW) Pty Ltd., an Australian company, certifies that it is the assignee of the entire right, title and interest in the patent application identified above by virtue of either:

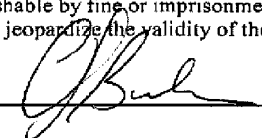
- An assignment from the inventor(s) of the patent application identified above, which is being recorded concurrently herewith pursuant to 37 CFR 3.11, a copy of which is attached hereto.
 OR
- An assignment from the inventor(s) of the patent application identified above. The assignment was recorded in the Patent and Trademark Office at Reel _____, frame _____.
 OR
- A chain of title from the inventor(s) of the patent application identified above to the current assignee as shown below:
1. From _____ To: _____
 The document was recorded in the Patent and Trademark Office at Reel _____, frame _____, or a copy thereof is attached.
 2. From _____ To: _____
 The document was recorded in the Patent and Trademark Office at Reel _____, frame _____, or a copy thereof is attached.
- Additional documents in the chain of title are listed on a supplemental sheet.

The undersigned has reviewed the assignment or all the documents in the chain of title of the patent application identified above and, to the best of undersigned's knowledge and belief, title is in the assignee identified above.

The undersigned (whose title is supplied below) is empowered to act on behalf of the assignee.

I hereby declare that all statements made herein of my own knowledge are true, and that all statements made on information and belief are believed to be true; and further, that these statements are made with the knowledge that willful false statements, and the like so made, are punishable by fine or imprisonment, or both, under Section 1001, Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Signature



(Day/month/year)

Date:

19.5.2006

Name:

CHRISTOPHER BURKE

Title:

MANAGING DIRECTOR

1205071 (Power_of_Attorney w chain of title): smc

Remote Entry System

Inventors: **Burke; John Christopher;** *(New South Wales, AU)*

Description

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation patent application of U.S. Non-Provisional Application No. 10/568,207 for REMOTE ENTRY SYSTEM, filed June 04, 2008, the disclosure of which is incorporated by reference in its entirety.

FIELD OF THE INVENTION

[0001] The present invention relates to secure access systems and, in particular, to systems using wireless transmission of security code information.

BACKGROUND

[0002] FIG. 1 shows a prior art arrangement for providing secure access. A user 401 makes a request, as depicted by an arrow 402, directed to a code entry module 403. The module 403 is typically mounted on the external jamb of a secure door. The request 402 is typically a secure code of some type which is compatible with the code entry module 403. Thus, for example, the request 402 can be a sequence of secret numbers directed to a keypad 403. Alternately, the request 402 can be a biometric signal from the user 401 directed to a corresponding biometric sensor 403. One example of a biometric signal is a fingerprint. Other physical attributes that can be used to provide biometric signals include voice, retinal or iris pattern, face pattern, palm configuration and so on.

[0003] The code entry module 403 conveys the request 402 by sending a corresponding

signal, as depicted by an arrow 404, to a controller 405 which is typically situated in a remote or inaccessible place. The controller 405 authenticates the security information provided by the user 401 by interrogating a database 407 as depicted by an arrow 406. If the user 401 is authenticated, and has the appropriate access privileges, then the controller 405 sends an access signal, as depicted by an arrow 408, to a device 409 in order to provide the desired access. The device 409 can, for example, be the locking mechanism of a secure door, or can be an electronic lock on a personal computer (PC) which the user 401 desires to access.

[0004] A proximity card can also be used to emit the request 402, in which case the code entry module 403 has appropriate functionality.

[0005] Although the request 402 can be made secure, either by increasing the number of secret digits or by using a biometric system, the communication infrastructure in FIG. 1 is typically less secure. The infrastructure 400 is generally hardwired, with the code entry module 403 generally being mounted on the outside jamb of a secured door. In such a situation, the signal path 404 can be over a significant distance in order to reach the controller 405. The path 404 represents one weak point in the security system 400, providing an unauthorised person with relatively easy access to the information being transmitted between the code entry module 403 and the controller 405. Such an unauthorised person can, given this physical access, decipher the communicated information between the code entry module 403 and the controller 405. This captured information can be deciphered, replayed in order to gain the access which rightfully belongs to the user 401, or to enable modification for other subversive purposes.

[0006] Current systems as depicted in FIG. 1 utilise a communication protocol called "Wiegand" for communication between the code entry module 403 and the controller 405. The Wiegand protocol is a simple one-way data protocol that can be modified by increasing or decreasing the bit count to ensure uniqueness of the protocol among different security companies. The Wiegand protocol does not secure the information being sent between the code entry module 403 and the controller 405.

[0007] More advanced protocols such as RS 485 have been used in order to overcome the vulnerability of the Wiegand protocol over the long distance route 404. RS 485 is a duplex protocol offering encryption capabilities at both the transmitting and receiving

ends, i.e. the code entry module 403 and the controller 405 respectively in the present case. The length of the path 404 nonetheless provides an attack point for the unauthorised person.

[0008] Due to the cost and complexity of re-wiring buildings and facilities, security companies often make use of existing communication cabling when installing and/or upgraded security systems, thereby maintaining the vulnerability described above.

SUMMARY

[0009] It is an object of the present invention to substantially overcome, or at least ameliorate, one or more disadvantages of existing arrangements.

[0010] According to a first aspect of the present invention, there is provided a system for providing secure access to a controlled item, the system comprising:

[0011] a database of biometric signatures;

[0012] a transmitter subsystem comprising: [0013] a biometric sensor for receiving a biometric signal; [0014] means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and [0015] means for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth.TM. protocol, and a WiFi.TM. protocol; and [0016] a receiver sub-system comprising; [0017] means for receiving the transmitted secure access signal; and [0018] means for providing conditional access to the controlled item dependent upon said information.

[0019] According to another aspect of the present invention, there is provided a transmitter sub-system for operating in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a receiver sub-system comprising means for receiving a secure access signal transmitted by the transmitter sub-system, and means for providing conditional access to the controlled item dependent upon information conveyed in the secure access signal; wherein the transmitter subsystem comprises: [0020] a biometric sensor for receiving a biometric signal; [0021] means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and [0022]

means for emitting the secure access signal conveying said information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth.TM. protocol, and a WiFi.TM. protocol.

[0023] According to another aspect of the present invention, there is provided receiver sub-system for operating in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute, and means for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth.TM. protocol, and a WiFi.TM. protocol; wherein the receiver sub-system comprises; [0024] means for receiving the transmitted secure access signal; and [0025] means for providing conditional access to the controlled item dependent upon said information.

[0026] According to another aspect of the present invention, there is provided a method for providing secure access to a controlled item, the method comprising the steps of:

[0027] receiving a biometric signal;

[0028] matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute;

[0029] emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth.TM. protocol, and a WiFi.TM. protocol; and

[0030] providing conditional access to the controlled item dependent upon said information.

[0031] According to another aspect of the present invention, there is provided a method for populating a database of biometric signatures in a system for providing secure access to a controlled item, the system comprising said database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, and means for emitting a secure access signal, and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon

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.