Accessible Authentication via Tactile PIN Entry

Travis Deyle, Volker Roth

German Abstract

Personal Identification Numbers (»PIN«) sind der Standard im Bereich der Authentifizierung von Kontoinhabern gegenüber Bankautomaten. PIN werden zunehmend von sogenannten shoulder surfers bei ihrer Eingabe erspäht. In Zusammenhang mit dem skimming oder dem Diebstahl der zugehörigen Debit-Karte ermöglicht dies Unbefugten Zugang zum Konto des Inhabers. Wir haben ein Verfahren zur Eingabe von PINs entwickelt, das Sicherheit gegen shoulder surfing bietet, und unsere Untersuchungen desselben an anderer Stelle bereits beschrieben. Das Verfahren erfordert jedoch ausreichendes Sehvermögen und benachteiligt daher zum Beispiel Blinde. In diesem Artikel präsentieren wir eine taktile Variante unseres Verfahrens und den Prototypen des zugehörigen Eingabegerätes. Das taktile Verfahren ist prinzipiell für Blinde geeignet und würde perfekte Sicherheit gegen shoulder surfing bieten, sogar wenn der Eingabeprozess vollständig mit einer Kamera erfasst würde.

Introduction

Personal Identification Numbers (»PIN«) are the standard means of authenticating oneself when withdrawing money from Automatic Teller Machines (»ATM«). Typically, a user proves herself to a machine by swiping a debit card followed by entering a four digit PIN number using a PIN pad with a three by four key matrix.

However, anyone who has the PIN pad in his field of view may observe the PIN number that a prover enters and use that information to impersonate the legitimate user. This particular attack is widely known as shoulder surfing. Furthermore, fraudsters steal or skim valid cards with increasing sophistication causing significant damage to customers and the banking industry.

In order to prevent shoulder surfing, we developed a Patent pending mechanism that allows entering one's PIN securely even if all input and output is performed in plain sight of a shoulder surfer [1, 2]. Blind persons would not benefit from the mechanism because it requires responses to visual output. Below, we describe an application of the underlying principles to a tactile PIN entry mechanism that can be operated without visual output. We built a prototype device for the mechanism, which we intend to use in usability studies of our mechanism.

Tactile PIN Entry

The tactile PIN entry mechanism requires palpable actuators that can be controlled by a computer process. In our prototype, we use solenoids with pins that can be raised or lowered by applying an electric current to the embedded electromagnet. Overall, eight solenoids are required, four per hand. Users position their index, middle, ring and pinky fingers

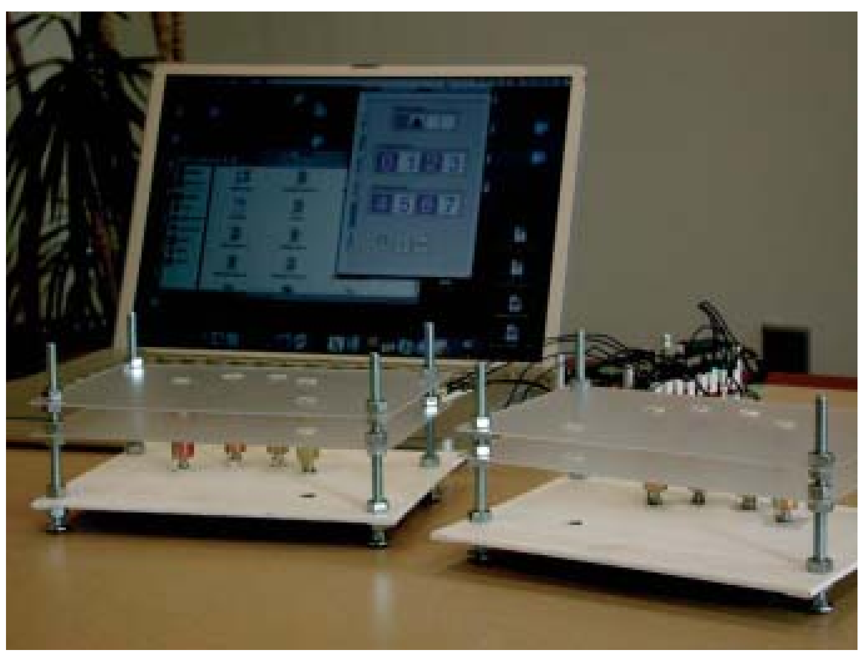

Figure 1: Shows the prototype setup with monitoring interface in the background. Response buttons are not shown.

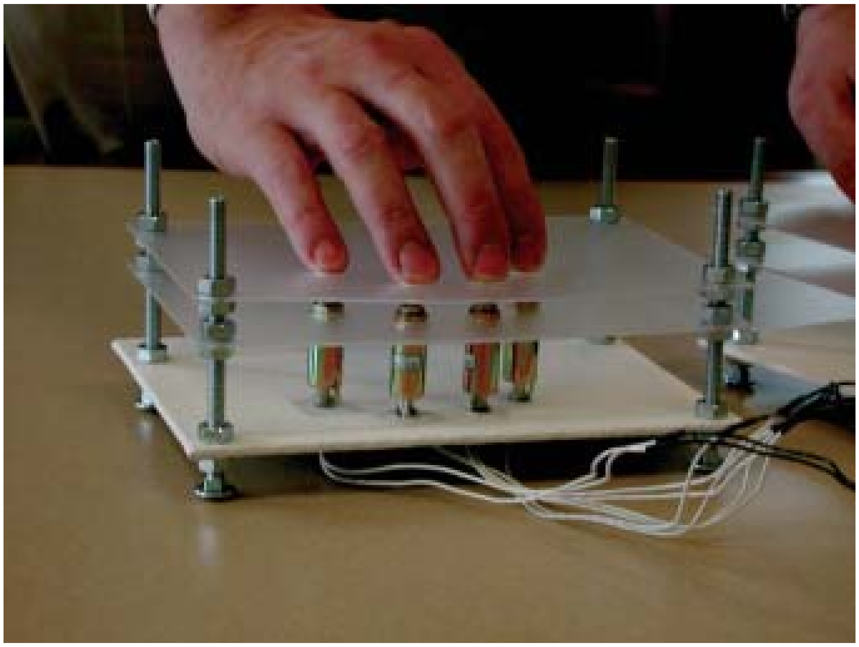

Figure 2: Users position their fingers over the solenoids and feel whether individual solenoid pins are raised or lowered.

over the solenoids such that they can feel whether a pin is lowered or raised. The thumbs are positioned over two buttons which signify either »raised« or »lowered«.

A PIN number consists of a sequence of fingers, for example left index, right ring, left index and left middle finger. The device begins by raising four pins. If the pin under the left index finger is raised then the user presses the »raised« button, and presses the »lowered« button otherwise. The device continues by raising a different set of four pins, followed by another response of the user. After three rounds, the computer can uniquely determine that the left index finger was »input« by intersecting the sets of pins that were in the indicated states in each round. The overall procedure is repeated for the next finger and so forth until all fingers are input.

With only the button presses being perceivable, a shoulder surfer gains no information about the entered PIN. Unless the positions of the solenoid pins can be measured as well, the device offers perfect secrecy even if the entire process is recorded by a camera.

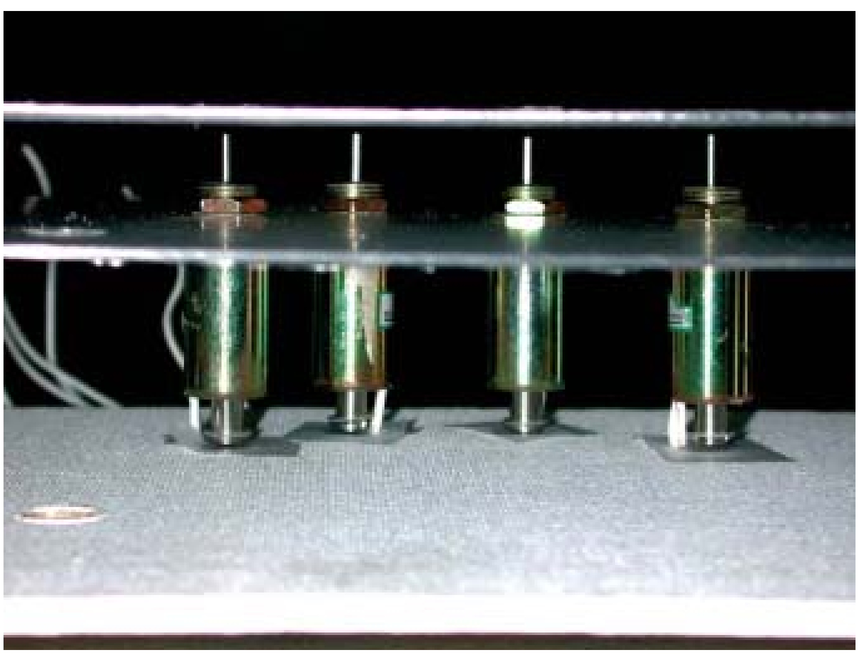

Figure 3: Solenoids are mounted on the middle layer which consists of a thin Plexiglas sheet. When raised, the pins protrude from the top layer by a small amount.

Prototype Device

We built a device to mount the solenoids such that users can conveniently position their fingers over them (see figure 2). The device consists of a sturdy cardboard layer at the bottom and two Plexiglas sheets on top, held in place by screws in the four corners. The solenoids are mounted on the middle layer such that the raised pins protrude a small distance from the top layer (see figure 3). We used two separate devices, one for each hand. The entire assembly is shown in Figure 1 with the controlling computer in the back.

The device interfaces with the computer through a hand-wired controller board that communicates with the computer via a USB connection (see figure 4). We used the PIC18F452 microcontroller from Microchip, which features 32 Kbytes of Flash program memory, 1536 bytes of RAM and 36 I/O lines. It was programmed in assembly using Microchip's MPLAB and In-Circuit Debugger and Programmer. The microcontroller was connected to the FT245BM, a USB controller that communicates to a PC via a virtual COM port. The eight push-type solenoids were driven by two L293DNE quad half H-bridges. The H-bridges accepted control signals at the +5V level from the microcontroller and then turned them into drive signals, supplying up to 600 mA to each solenoid, at the +12V level.

Lesons Learned

Ultimately, we showed that such a setup could function, but there were a few soft-spots in the design. First, the power regulator had a tendency to overheat after extended use, as did the L293DNE half H-bridge chips. Further, programming in assembly was too time-consuming and error-prone. Also, the microcontroller required a manual reset-on-powerup - this just isn't practical on a device in the field. Finally, the original design was wire-wrapped onto a prototyping board, making it unacceptable for quick turn-around of new boards. To address these issues, a new board has been constructed.

It uses the PIC18F45J10 microcontroller and the FT232R USB controller. Both of these devices offer superior capabilities to their earlier counterparts and at lower unit costs. The microcontroller is programmed in C using Microchip's MPLAB IDE and C18 compiler. Code is again loaded into the microcontroller via the In-Circuit Debugger and Programmer. The power for the controllers is +3.3V, regulated off of the USB power supply. A voltage-supply monitor was also added to automatically generate the power-on-reset to the microcontroller. Each solenoid driver now consists of a NMOS transistor, supplying up to 750mA at up to 60V, and Schottky diodes to suppress solenoid back-EMF. The new design was produced using Cadsoft's Eagle program for schematic entry and PCB board layout. The design utilizes entirely surface mounted components, making the PCB very small at 1.5 x 2.5. The PCB was manufactured by PCBexpress. The new board addresses all of the soft-spots in the old design and also adds a unique feature – the FT232R has a built-in unique ID, making it useful for dongled applications. This may make cryptographic PC-device authentication possible over the USB port.

Preliminary Conclusions

We built a tactile PIN entry device that uses computer-controlled solenoids as palpable actuators. Users enter their PIN as a sequence of fingers by responding to raised and lowered solenoid pins. Responses consist of button clicks with the thumbs, which indicate whether the pin under the current PIN finger is raised or lowered. Based on our experiences with the first prototype we built an improved PCB for the second generation controller. We intend to use the device to perform usability studies of our PIN entry mechanism. In a commercial-grade implementation, the mechanism would offer perfect security against shoulder surfers even if the entry procedure is recorded with a camera. Moreover, the mechanism can be operated by blind persons. If found usable, the mechanism could improve the accessibility of ATMs for handicapped people.

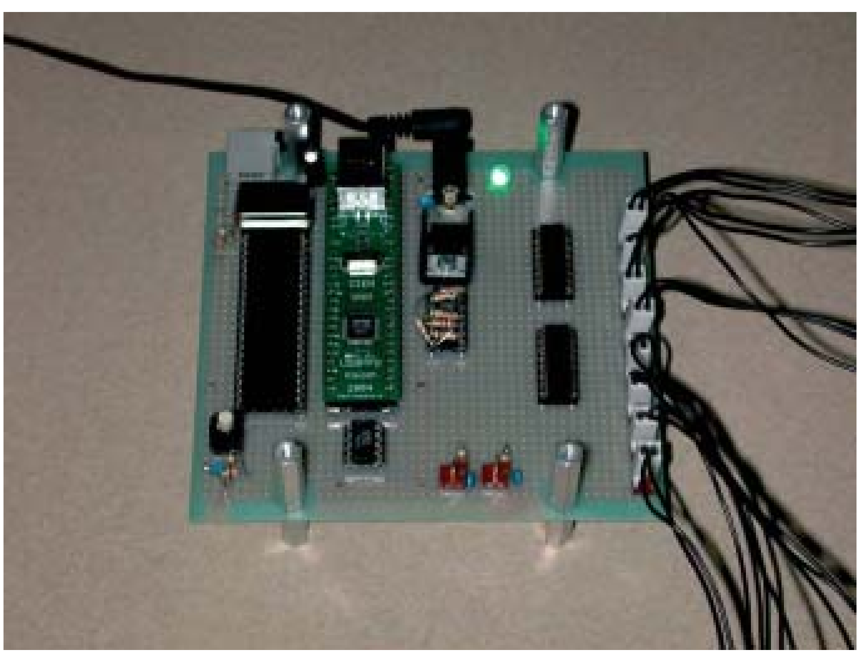

Figure 4: The solenoids are controlled through a PIC board that is connected to the host computer via a USB (USB cable not shown).

References

[1] Volker Roth. Security meets usability: Entering one's PIN in a public space. Computer Graphics Topics, 17:24-25, April 2005.
[2] Volker Roth, Kai Richter, and Rene Freidinger. A PIN entry method resilient against shoulder surfing. In Proc. 11th ACM Conference on Computer and Communications Security, Washington, DC, USA, October 2004.

Point of Contact

Dr.-Ing. Volker Roth
OGM Laboratory LLC, Omaha, Nebraska, USA
E-mail: vroth@ogmlabs.com, volker.roth@acm.org