“On-Card” User Authentication for Contactless Smart Cards based on Gesture Recognition

Markus Ullmann\textsuperscript{1, 2}, Ralph Breithaupt\textsuperscript{1}, Frank Gehring\textsuperscript{1}
\textsuperscript{1} Federal Office for Information Security
53133 Bonn
www.bsi.bund.de
\{markus.ullmann, ralph.breithaupt, frank.gehring\}@bsi.bund.de

\textsuperscript{2} University of Applied Sciences Bonn-Rhine-Sieg
www.h-brs.de

Abstract: Smart cards are widely used for security purposes. To protect smart cards against misuse an authentication process (e.g. entering a pin or password) is necessary. Due to missing input interfaces “on-card”, an external terminal is required to input the password. Unfortunately the required external hardware (e.g. keypads, etc.) opens up new security issues by being vulnerable against attacks like side channel, forgery & tampering, man in the middle, eavesdropping and others. An elegant solution for such problems is an authentication process “on-card” without the need for external devices.

This paper presents a new class of contactless, ISO 14443 compliant smart cards which are equipped with a multipurpose user input interface as 2D gesture recognition sensor together with an optical feedback component. This offers new “on-card” authentication, card configuration and even front end interface capabilities. We will describe the basics of the general hardware design and discuss the gesture recognition process.

1 Introduction

Today, smart cards are primary used as security token. To avoid misuse of the smart cards it is common to implement an user authentication. For this biometrics or passwords are used. If the capturing of the biometric information or the passwords for user verification takes place on an external terminal the verification data has to be transfered to the card using an authenticated and secured communication channel. Even in this case skimming of the verification data on an external terminal is a considerable security issue. Skimming of the verification data can be principally avoided if the password is directly captured on an input component of the smart card itself. Here, we describe a first contactless smart card prototype with an input interface. This contactless card is equipped with an ISO 14443 interface, a security controller (here smartMX [NXPb]) and in addition with a capacitive 2D gesture sensor for the collection of human gestures “on-card” as well as an optical component to provide necessary feedback to the user.

The idea to integrate human input and output devices in smart cards is not quite new. In [Ull07] smart cards with an integrated display are introduced. Also [J. 09] suggested an
ID-card with a display component. Moreover, smart cards with an input interface have been discussed, see [VIS08] or [UV10]. The last one suggested key button components for the acknowledgement of transactions on-card. [VIS08] presented the integration of a number key pad. Novel is the integration of a gesture input component in combination with a feedback component, as described in this paper.

Here, we propose to use gestures “on-card” mainly for cardholder verification.

A gesture is a movement with time behaviour. A good distinction of gestures is given in [WH99] by Wu and Huang. They distinguish

1. gestures for human communication
2. gestures for human conversation
3. gestures for human interaction with virtual objects and
4. gestures used in user interfaces for the control of systems

Here, we mean gestures of the last type. First of all in a 2D scenario, a gesture can form a number and can be collected and processed on-card. But we show, that gestures are not restricted to numbers or characters. From a theoretical perspective only the construction of the sensor restricts the diversity of useable gestures for user authentication.

The rest of the paper is organized as follows: Section 2 starts with a description of related work. A common usage of gestures is for the control of game consoles, smartphones and touch panels. In this section known usages of gestures for human authentication are presented. Section 3 presents the principal construction of the contactless card with a capacitive gesture input component and its properties as basis for gesture recognition. Basis for the technical presentation in this section is a first prototype which is build in cooperation with NXP based on requirements of the authors. The next section 4 describes the “on-card” human authentication process. In the following section 5 a brief security analysis is given. Finally, section 6 summarizes the findings of this paper and gives an outline of open security issues regarding gesture authentication.

2 Related Work

Within the last 3 decades a wide variety of 2D gesture recognition algorithms have been developed for many different applications on mobile devices like online handwriting recognition, symbolic textural input or intuitive device control. To date, it became the established usage concept for devices with touch panels, especially for smartphones, see [Pal11], [App]. As the next step current research and development activities focus on 3D-gestures recognition based on camera systems, acceleration sensors and others not only as a user interface for game consoles but as a new paradigm for human machine-interaction in general.

Gestures as authentication mechanisms were published first in [PPA04]. Patel et al. suggested a gesture-based authentication scheme for untrusted public terminals. Farella et al.
proposed gestures as personal verification system for PDAs. They used biometric signatures based on tri-axial accelerometers integrated in the PDA, see [FOBR06]. In [KYJ+10] Ketabdar et al. proposed 3D signature gestures for user authentication of mobile phones. At last Chong et al. [CM09] discussed discrete gestures as alternative to alphanumerical characters in passwords, first. But they neither published a concrete alphabet nor did they present an entropy calculation.

A good overview of character recognition can be found in [Cha90] and [Cha98]. A segmentation algorithm for the isolation of strokes is described in [MB99], [Don09] and an interesting contour feature algorithm in [Ver03]. [Thi97] specified a character recognition procedure which combines segmentation-based and segmentation-free recognition methods. [YMS+99] addresses the usage of additional velocity features for character recognition.

3 Hardware Concept for “On-Card” Authentication with Gesture Recognition

Although 2D gesture recognition is an integral part of millions of smartphones, it is still very challenging to develop and integrate the necessary hard- and software into a contactless card. Due to the general application requirements, the standardized form factor and the limited resources of a contactless card, all additional components and features are subject to the following constraints:

- **low power**: The available power by field induction for all components on our prototype is about 50 - 70 mW.
- **low profile**: In order to meet the ISO-standard for the maximum thickness of a card all components should be far less than 0.3 mm in height.
- **mechanically robust**: The cards still have to meet the standardized requirements for mechanical flexibility and robustness. This means the whole card has to be robust against bending and torsion as well as dirt and splash water.
- **low computing capability**: Although the performance per Watt ratio and the available memory of suitable microcontrollers are continuously increasing the computing capability will always be at the very low end of the spectrum. Therefore active power management as well as algorithm efficiency are essential for all software concepts.

Since our approach does not use any external hardware except the simple card reader, the proposed “on card” interface must provide all the components needed for a functional, reliable and intuitively controllable mode of operation. Desirably the operating concept should be as publicly acceptable as possible. Therefore we do not only need a gesture input sensor but also a distinctive optical feedback component to inform the user about the current state of the card and the success of the gesture recognition process in particular.

Figure 1 depicts the necessary smart card components. In the following we describe the
solution we have developed in our feasibility study that resulted in a working functional prototype.

3.1 Construction of a 2D Gesture Sensor

In our study we found that the easiest and most reliable way to implement a 2D “on-card” gesture input sensor is the use of a capacitive touch matrix (see figure 2 and [Har]) printed on the inlay PCB (printed circuit board) of the contactless card. With an array of 4 x 4 sensor pads we achieved a sensor area of 40 x 40 mm. By using an adaptation of a “center of mass” algorithm we can calculate the position of a finger-sensor contact with a resolution of around 6 - 7 bit (so between 64 and 128 distinguishable positions for each axis or about 80 dpi). With a sampling time per position estimate of 16 - 30 ms we support a minimal overall speed of 0.7 characters per second for complex characters (e.g. 1.5 s to enter a “Z” or a “8”, consisting of 48 - 64 detected position samples). With fewer samples per character higher speeds are possible.

3.2 Gesture Recognition Processing

Our prototype system is based on a standard smartMX ISO 14443 compliant communication & security controller with a JavaCard2.2-operating system. However, for position data acquisition, filtering and the gesture recognition we needed a more flexible processing unit and added an Arm Cortex M0 controller [ARM11](running at 6 - 12 MHz). This ultra low power processor has proven capable enough to recognize even complex, time
dependant gestures without a noticeable delay and a feasible first detection rate of $\sim 90\%$ (numbers and characters).

This solution can support a wide variety of the different known 2D gesture recognition algorithms (all the pixel-, vector- and sensor histogram based approaches mentioned in section 2) as long as they have low to moderate requirements for computational power and memory capacity.

### 3.3 Optical Feedback Components

Developing display components that meet the above mentioned requirements for contactless cards is still a topic of current research and development. In order to provide different solutions for the requirements of various application scenarios regarding the potential for feedback information and cost constraints, we implemented two different concepts for optical user feedback.

#### 3.3.1 Segment EInk-Display

As a very comfortable feedback component we used a 10 character, 14 segment per character EInk-display [Ein11]. With this display type a very high level of user interaction is possible: all standard characters and numbers as well as simple symbols can be shown as requests or as feedback to the user. With such a device even an application with a complex menu structure is possible in which the user can navigate by using simple control gestures. Unfortunately those displays are still a little slow, relatively expensive and can not display
all possible gestures. Apart from the used EInk-technology there are current developments that provide very cheap printable segmented displays as well as different matrix display types that are suitable for the future generation of contactless cards.

3.3.2 LED Matrix

A very flexible and also a relatively inexpensive way to give gesture related feedback to the user is a LED matrix embedded in the touch sensor area, see figure 2. Even with a minimal set of 3 x 3 LEDs (or similar/maybe printable illumination techniques) it is possible to reenact the entered user gesture, display a randomly generated gesture set to the user or give simple position feedback while entering a gesture for a surprisingly large number of different gestures: all numbers and characters and even more symbols can be displayed as a sequence of 9 illuminated spots. If a matrix of 5 x 5 or more can be implemented, the number of displayable gestures increase dramatically. Additional single LEDs can also be used as fixed feedback components such as status or error signals.

4 “On-Card” Authentication

4.1 Password Authentication

An authentication procedure based on gestures is very easy to learn and similar to a normal password verification process. Precondition is that a contactless card and the card holder
share a secret password. This password is chosen at random during the personalisation of the card and securely issued to the card holder. During a verification of the card holder he has to input his password. Now, the user has to input the sequence of corresponding gestures for each digit of the password, see figure 3. Therefore the user is guided by the card itself. After each gesture input, collection and digit recognition a short feedback is given to the user according the detection of a known digit. After a complete gesture input the inserted password is compared with the reference password stored on the card. In case of a full correlation the user authentication is successful which can be shown to the user on the display or as a specific symbol on the LED matrix.

4.2 Gesture Alphabet

Beyond the recognition of digits gesture collection components permit the collection and recognition of arbitrary graphical inputs. The use of shared secret graphical gestures is briefly suggested as alternative to the usage of passwords. Gestures are proposed to improve password usability. Graphical passwords exploit the picture superiority effect [DNW76]. Cognitive studies have shown that people can recognize graphical information much better then alphanumerical [CM09]. Here, we pick up this cognitive human property.

Gesture alphabet means, that a set of basic gestures is defined similar to numbers or characters. In that case an individual authentication gesture consists of a sequence of elements of the gesture alphabet just like passwords which consists of a sequence of numerical or alphanumerical characters. Figure 4 gives only a notion of possible elements of a gesture alphabet. Obviously, the set of gesture elements is much larger then the quantity of alphanumerical characters. So, the entropy of one element of the gesture alphabet is much higher in contrast to an element of the set of alphanumerical characters. One benefit is a possible reduction of the password length without loss of security, if a gesture alphabet is used instead of digits or alphanumerical characters. A further benefit of using secret gestures instead of numbers or characters is that the human capacity of remembering them is much better compared to numbers respective characters, as mentioned before.

In principal, gesture authentication can be done either on basis of a defined gesture alphabet as describe before or on individual complex gestures with high entropy. But a precise definition and description as well as an entropy consideration is not subject of this paper.

Although gestures are well known in smartphones current users of smart cards are not familiar with this kind of mechanism to date.

An authentication procedure is very easy and similar to a normal password verification process. Now, precondition is that a contactless card and the card holder share a secret gesture. This gesture is chosen at random during the personalisation of the card and securely issued to the card holder. During the verification of the card holder he has to input the secret gesture at the gesture collection component. Next, the recognised current gesture and the stored reference gesture are compared. In case of correlation the authentication is successful.
4.3 Examplary Number Insertion Process

Here, we describe a password insertion process of a password consisting of four digits, e.g. “9137”. Due to the number insertion based on gestures following situation can occur:

1. inserted digit is recognized correctly (correct recognition)
2. no digit is recognized (alikeness value of the collected gesture to each registered reference digit is too low)
3. false digit recognition (false recognition)

Now, in contrast to the use of a pin-pad, false number recognition of an inserted number is possible. We regard false recognition in our usage concept. In addition to digit gesture recognition a control gesture is defined. Here, only a horizontal stroke is specified. A human stroke gesture indicates an erasure of the last input digit. Figure 3 illustrates a password insertion process. Here, two numbers was already recognized and covered (picted as “-” and “-” in the display). Just the currently recognized gesture input is shown (“3”) by the card for a very short time. This is a necessary feedback to the user to interact if the gesture recognition of the card was not correct. In this case the user has to perform a horizontal stroke to erase the last digit. If no stroke is inserted after a number recognition within the time interval $\Delta t$ the next digit input is requested. When the last digit of the password is recognized the password verification process is performed and the user is informed of the failure or success of the password authentication.
5 Brief Security Analysis

Here, we observe only an external attacker. So, invasive attacks of smart cards are excluded as well as side channel analysis of the number insertion on the capacitive sensor element.

5.1 Password Skimming

Today, password skimming on external terminals is a known attack for smart cards as described in section 1. Insertion of passwords on-card, as proposed in this paper, prohibits this attack in general. But the use of gestures for the insertion of numbers raise the problem of recognition errors in contrast to the use of a key pad.

5.2 Gesture Attack

As mentioned in section 4.3, following situations can occur during a number insertion and recognition procedure:

1. inserted digit is recognized correctly (correct recognition)
2. no digit is recognized (alikeness value of the collected gesture to each registered reference number is too low)
3. false digit recognition (false recognition)

In principle, comparable to other defective inputs, like biometrics, false number recognition is not completely avoidable. We cover this false number recognition with a feedback concept, as described in section 4.3. The smart cards react to each individual number insertion with a short feedback of the recognized number to the user. This is essential for a genuine card holder to verify that the smart card has performed a correct number recognition. A password verification itself is only performed after a complete insertion of a password and not after each number insertion.

The requirement for the feedback concept is, that a false digit recognition may not allow an active attacker, who is in possession of a contactless card, to reduce the available password space for an active online brute force attack of the password. We recommend that a card responds to a digit insertion with a feedback to the user without discharging any information concerning the right password. That is the case if the card is in possession of an attacker, too. But a verification of the password is performed not until the whole password is inserted. So, an attacker can not take an advantage of a false number recognition.
5.3 Distant Gesture Insertion

One attack method which is not yet completely investigated is the input of the password from a distance, known as pocket attack. Our smart card is equipped with a capacitive gesture input component. A finger touch of the sensor component effects a local capacity modification which is sensed and exploited by the card. The sensor component measures only the described effect. In general it can not distinguish whether the capacity modification is achieved by a touch of a human finger or in a different way. A pocket attack denotes that a contactless smart card is activated by an attacker terminal (e.g. example in a public bus) whereas the smart card is in a users pocket and the attacker performs gesture insertion attempts. We assume that a correct password insertion is not likely. But any distance gesture insertion can be used to enforce wrong password verifications and disable the smart card anyhow.

To hinder that kind of attack an additional user interaction phase randomly chosen by the card and shown in the feedback component to the user has to be performed prior to the password insertion. This operation can be understood as an explicite “switch-on” of a contactless card. An attacker can not see the chosen random gesture displayed on the feedback component. If this gesture is not inserted during a defined time interval $\Delta t$ the card is moved in a configured short sleep mode.

Here we have to point out, that an activation of a contactless card according ISO 14443 is only possible within a very restricted distance between the terminal and the contactless card, see [NXPa]. Moreover, an activation is a precondition for a gesture collection anyway.

5.4 Latent Finger Marks

Every touch of a finger on a plane surface usually leaves latent finger prints, every swipe movement leaves tracks that can be easily made visible by an attacker to determine the last performed gesture. So, the described effect can appear on our cards as well. As a possible countermeasure we could use surface materials that repel finger marks. This technique can reduce this effect. Alternatively, the user should perform a swiping gesture after each password insertion.

6 Conclusion

Here, we propose to enhance contactless smart cards with a 2D gesture collection component. This component is used for the insertion and recognition of human inputs. First of all, this component can be used for the input of digits performed as gesture. From a security perspective, this component can be used for human password insertion and card holder verification on-card. Our concept prevents user to input passwords for card holder verification on external terminals. We conclude, that this technology avoids skimming of
passwords on external input devices.

Moreover, we showed briefly that gestures as such can be used for authentication purposes. Here, we have only given a brief introduction to gesture authentication based on number gestures. But we showed that this component allows arbitrary gestures for authentication purposes. Only the recognition accuracy of sensor elements in combination with the recognition algorithms restrict the complexity and number of useable gestures. Here, a new research area is arising. This includes social studies regarding the human capacity for remembering gesture based secrets and the consumer acceptance of gesture authentication on smart cards.

As a consequence of our brief security analysis further detailed technical examinations have to be performed by analyzing the real attack potential of side channel analysis and distant gesture insertion.

7 Acknowledgement

We thank our colleague Christian Wieschebrink for his valuable remarks.

References

[App] Apple Computer Inc. A portable communication device with multi-touch input which detects one or more multi-touch contacts and motions and performs one or more operations on an object based on the one or more multi-touch contacts and/or motions. US patent, US 2007/152984.


On-Card User Authentication for Smart Cards based on Gesture Recognition


[NXPa] NXP Semiconductor. ISO/IEC 14443 Eavesdropping and Activation Distance, 13.56 MHz Proximity Smart Cards, Application Note. Rev. 1.01, January 2008.


