'PRESSURE SEQUENCE' - A NOVEL METHOD OF PROTECTING SMART CARDS

Neil Henderson and Pieter Hartel
Department of Electronics and Computer Science, University of Southampton, Highfield, Southampton, SO17 1BJ, United Kingdom.
N.Henderson@ecs.soton.ac.uk, P.H.Hartel@ecs.soton.ac.uk

Abstract If someone knocks on your door, the chances are that you can tell by the sound who it is. This simple idea is the basis of our pressure sequence method, which records the signal arising from a user tapping on a smart card. We have built a prototype, piezoelectric, screen printed pressure sensor on a smart card. We have also conducted an experiment with 34 volunteers to assess the effectiveness of the pressure sequence as an identification method. While the Equal-Error Rate (EER) of our current system is too high, we have identified a number of improvements that will lower the EER and make the identification more accurate. The sensor and associated circuitry are inexpensive, making it feasible to embed our technique in medium to high-end smart cards.

Keywords: Smart cards. Personal Identification. Biometrics.

1. INTRODUCTION

The security of an information system depends to a large extent on its ability to authenticate legitimate users. Other factors are also important, such as the ability of the information system to withstand attacks of various kinds. However, we will only be concerned with authentication. The most powerful authentication schemes have three components [9].

1 The token: something the user owns.

2 Knowledge: something the user knows.

3 Biometrics, something:

- The user is (i.e. physiological properties such as fingerprint, retinal pattern)
- The user can do (i.e. behavioural patterns arising when signing, speaking, walking).

Smart cards are in widespread use as the 'token', and pin codes are ubiquitous as the 'knowledge'. Biometrics are not (yet) in widespread use, for reasons of cost, but also for reasons of social acceptability. However, this situation is beginning to change. Jain et al survey a number of large biometric security projects that are currently in progress [8]. They also lay down the ground rules for biometrics that are useful to existing and emerging e-applications. A biometric should be socially acceptable, low cost, accurate and quick. Our work offers a novel, inexpensive and socially acceptable biometric that is fun to work with. The accuracy of our method is not yet adequate, but we are working on improvement.

Carelessness and other operational mishaps [2] can defeat many security schemes. For example, PIN numbers and Passwords can be forgotten or discovered by malevolent third parties. Making matters worse, it has been estimated that around one quarter of all card owners actually write their PIN digits on the card! [15]. For low value debit transactions, such as for using a public phone or for a transportation card, presentation of the card itself is deemed sufficient for the transaction to occur. Since the value of the card is typically small, loss results in little more than irritation for the owner, and there is little incentive for theft. However in a multi-application scheme, many such applications may be active, thereby increasing the card's value, hence its attractiveness to a thief. As smartcard processors become more powerful, their capacity for running more applications and storing significant amounts of data increases [17]. Following this trend, the card's potential value to a user increases, and hence there is an increased requirement for protection of access to the smart card contents.

This paper discusses the requirements and constraints of a novel sensor that measures a behavioural trait, and uses the measurements to verify the identity of the smart card user. The next section reviews some of the current methods for achieving similar goals.

2. RELATED WORK

Currently there exist a number of methods of restricting the use of a smartcard to its legitimate owner. These range from Passwords, PIN numbers and signatures, to biometric methods of verification. They all rely upon the use of external devices for verification. For example, PIN numbers and passwords must be entered through an external keyboard, signatures must be written down, then verified by a (typically non-expert) third party. Biometric methods of verification are executed by the external capture of a characteristic, then the comparison of this live characteristic to a template stored on card. The comparison process of-

ten occurs externally to the card, and is subject to tolerances set within the comparison algorithm.

This combination of reference knowledge held on smartcard and the external capture and/or comparison of some quantity, is not designed to protect a smartcard's contents. Rather it is designed to protect access to an external service or facility. The smartcard plays both the roles of key and storage facility for a reference quantity. Such a scheme is not entirely applicable to the protection of a smartcard's contents. Firstly, multi-application cards would require either uniformity of external hardware (at each point of use) or each active application running on card would require a verification program tailored to the system at the points of use for that application. Secondly, if biometric verification occurs externally to the card, the external device determines the tolerance of the comparison algorithm. This, in effect, exposes a user's data to someone else's idea of security.

To circumvent these problems, we aim to incorporate all components of a verification system onto a smart card. In this way, the card's owner assumes responsibility for the protection of his data, and may select the tightness of security with a level appropriate to the value of the smartcard's contents and to his paranoia.

An alternative would be to embed the functionality of the smart card into a mobile device, such as a PDA or a mobile phone. Indeed mobile phones with a biometric (fingerprint) sensor have been announced. However, following this alternative route would require ATMs, POS terminals etc. to be upgraded so that they can communicate with the new, secure mobile devices, for example via a short range radio link, or infrared. The changes to the current world-wide infrastructure would require considerable investment, whereas our proposal requires no such changes.

To augment the capabilities of a smart card with a biometric sensor, one could integrate a commercially available fingerprint sensor on the card. Probably all commercial fingerprint sensors are silicon based, such as the STMicroelectronics TouchChip, the Veridicom FPS1000, or the Siemens Fingertip Sensor. These devices consist of a rectangular array of between 10,000 and 100,000 capacitance sensors. The chips are large, ranging from 200 to 1000 mm^2. The thinnest sensor (the Siemens) is 1.4 mm thick. To use these devices, the fingertip has to be placed on (protected) surface of the sensor. The Thomson CSF FingerChip is of a different design. It is a thermal sensor, which is used by sweeping the finger over a sensor 'strip'. This makes it possible to have a smaller array with only 820 sensors. The software then reconstructs the fingerprint. The silicon-based sensors are all too thick, too large (risk of breakage) and too expensive to be integrated with smart cards. Because of the high

resolution of (typically 500 DPI), silicon based sensors, with the associated software, offer False Acceptance Rate (FAR) and False Rejection Rate (FRR) typically less than a permille. Most commercial systems use a PC for the actual processing, making and verifications times in the order of a second possible.

Using a computer keyboard to verify identity on the basis of behavioural traits is attractive as keyboards are often already present. A system exploiting this would measure the 'rhythm' with which people type on keyboards. Joyce and Gupta [9] give an overview of early work on keystroke dynamics, showing that a keyboard based rhythm sensor can be effective, offering an EER in the order of 5-10%. Proposals have been made to apply this technique also to users typing on the keypads of ATMs, but we do not know whether any experiments have been done. We would expect that the typical sequences that users type on ATMs are to short to be useful [13].

Behavioural traits have some physiological basis, but also reflect a person's psychological state [12], as such behavioural biometrics will be influenced by the mood, emotion and environment, in which a person finds themselves. Examples of behavioural biometrics include; voice recognition [11], in which a spoken pass-phrase is sampled and compared to a reference template. Use of the pass-phrase, requires that both the voice characteristics and the spoken word match with the template. Dynamic signature analysis [6], is a method of identifying a person based upon the way in which a signature is created. It is insufficient for a forger to generate a signature which merely resembles a person's genuine signature, the dynamics of writing, such as pen pressure, duration and order of strokes are all accounted for in this method.

One characteristic of voice and dynamic signature biometrics, is that the person under investigation must want to be recognised. A behavioural biometric where this is not quite the case is gait recognition [7], based upon the way in which people walk, disguising gait is likely to draw considerable suspicion.

As a conclusion of this brief survey, we believe that we have justified why developing techniques to make the smart card itself more capable is worth while investigating. This will be the subject matter of the remainder of the paper.

3. SYSTEM CONSTRAINTS FOR AN ON-CARD VERIFICATION SYSTEM

A primary concern when discussing smartcards is cost. Components required for a proposed on-card verification system must be of low cost. In

addition, they must be both robust and reliable. For use on a smartcard, components should be sufficiently flexible to withstand the strains of normal smartcard use.

One technology which is compatible with the above is that of Polymer Thick-Film (PTF) [4]. The PTF technology is one in which materials are selectively deposited onto a substrate, typically, this is performed using a screen printing process. Common PTF materials include conductors, resistors, dielectrics and piezo-electrics, which together can produce devices with good sensing properties, robustness and be, importantly, of low cost and high mechanical flexibility [14, 16].

Since the verification algorithm must run on the card's processor, it should be as simple and efficient as possible. The next section describes a potential method of identity verification, which makes use of a simple PTF sensor and offers a reasonable level of discrimination, at low computational cost.

4. A DESCRIPTION OF THE 'PRESSURE SEQUENCE' METHOD

If someone knocks on your door, the chances are that you can tell by the sound who it is. In the early days of telegraphy, operators would identify each other by recognising the way in which they tapped out messages [12]. These simple ideas form the basis of our pressure sequence method. There are two different aspects to knocking on a door (or on a smart card for that matter). The first aspect is that of the actual rhythm. As anyone can choose a particular rhythm, this will not be a fraud resistant aspect to identify a person. The second aspect is that of the actual pressure exerted on the door/smart card during each of the different taps. We would argue that this aspect depends mostly on bio-mechanical properties, because these properties are determined by a complex biological system: the human hand has 19 bones, 19 joints, and 20 muscles with 22 degrees of freedom [10]. This offers considerable scope for a biometric that tries to distinguish between humans on the basis of finger, hand and wrist motion.

Our ultimate aim is therefore to differentiate people based on the actual pressure pulse from the 'knock' itself, not on the rhythm. If we can do this, identification will be independent of sequence, although the sequence may be incorporated to add a further layer of discrimination. This is analogous to voice recognition, whereby, recognition requires both the voice characteristics expressed through a pass-phrase, and the pass phrase itself. Another analogy is identifying people by the way they type on computer keyboards. Our work differs from keyboard behavioural

measurements in two essential aspects: firstly we measure not just on/off switches but complete pressure curves. This gives more detailed information. Secondly we do not rely on external infrastructure, such as keyboards. Our measurement apparatus is stand-alone.

Having discussed the foundation of the pressure sequence method, we now describe the experimental prototype sensor in the next section.

5. PROTOTYPE SENSOR

Our prototype sensor is a simple three-layered device, comprising of top and bottom electrodes sandwiching an active piezo-electric layer. Applied pressure causes proportional charge generation within the piezo layer. Charge is measured using a simple charge amplifier and ADC for now connected to a PC. The sensor is screen printed directly onto the smart card. The charge amplifier is capable of measuring small charges corresponding to gentle impulses on the smart card with the embedded sensor. The signal capture electronics could be packaged into an ASIC (and onto the smartcard), generating a small reduced signal template, for efficient comparison on the card's processor.

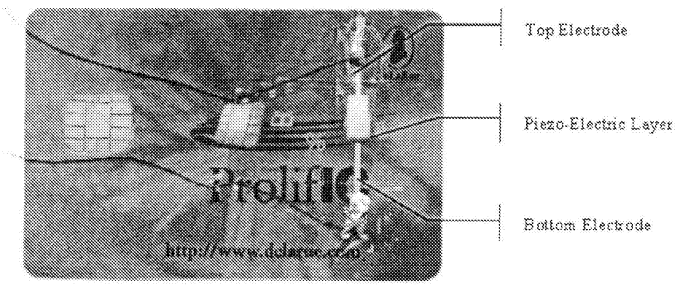

Figure 1 Smartcard with Embedded Pressure Sensor

We have experimented with one type of smart card (PVC). The cards we used were finished, complete with offset printing. A typical PVC card is thermally stable up to 80 °C [5]. However, our screen printing process heats it up to 130 °C. Whilst it is technically possible to work with PVC that remains stable at higher temperatures, the cost effectiveness of such an approach is questionable. An alternative smart card base material, Polycarbonate remains stable at temperatures up to 150 °C, but it is also considerably more expensive than PVC. Since the price of the actual plastic is a small fraction of the total costs of a smart card, it would

be possible to use materials that have high temperature stability. An alternative is to screen print the sensor on Mylar, and then to bond the sensor onto the card, for example during a lamination process. We will study the cost implications, and also investigate the implications for the offset printing and further processing steps, caused by possible unevenness in the card surface.

6. EXPERIMENTAL METHOD

To validate our biometric, we invited students and staff from our department to spend five minutes of their time doing an experiment. As one would expect, only a small number (34) of students and staff volunteered. The population is thus self-selected, rather than chosen at random. However, we believe that there is a reasonable variability in the population to make our experiments valid. Our number of volunteers is also comparable to that reported in other, similar studies [9]. Based on the outcomes of our initial experiment we plan to mount a larger scale experiment with a population that is representative for the population at large, and which is randomly selected.

Each volunteer was asked to choose a short tapping sequence (typically lasting between 2 and 4 seconds), and to tap that rhythm 30 times, in three groups of 10 sequences. In the first sequence the card was held in one hand whilst tapping with the other. In the second sequence, the card was held in place on a table with one hand, and in the third sequence, a mouse mat was placed between the card and the table. These three scenarios were thought to be representative of the way in which our system would be used in the real world, and remove some experimental bias. The volunteers were not given immediate feedback on how they were doing. Instead, they were asked to concentrate purely on tapping the rhythm. Our experimental set-up is able to give immediate, visual feedback, showing the waveform as it is tapped. However, we discovered in tryouts that this incited volunteers to vary their rhythms and the tapping motions to manipulate the visual cues. We felt that this created a distraction, and consequently disabled the immediate feedback.

Table A gives an indication of the property of the various rhythms chosen by our volunteers.

Volunteer	M/F	Age Group	# Taps	Sequence Duration (mS)	Shortest Interval (mS)	Longest Interval (mS)
ThomasF090200	M	41+	2	438	388	388
Marcus030200	M	26-40	3	1004	263	566
Paul	M	18-25	3	1357	360	890
Mauricio	M	26-40	3	980	417	424
Yavuz	M	26-40	3	1289	383	621
Lesley040200	F	41+	4	1324	277	342
Bob030200	M	41+	4	1706	318	665
Dan030200	M	18-25	4	1842	343	760
Jeff030200	M	26-40	4	1273	269	475
James030200	M	26-40	4	1298	237	492
Danny030200	M	26-40	5	1911	227	424
Yalin030200	M	18-25	5	2001	412	435
Yean030200	F	18-25	6	2342	311	654
Mark030200	M	41+	6	3395	253	993
Marijke	F	41+	6	2475	224	604
Theo040200	M	18-25	7	2602	223	705
Peter030200	M	26-40	7	3033	184	620
Uli030200	M	26-40	7	3551	252	972
Dave030200	M	41+	7	2513	216	537
Manabu	M	26-40	7	4274	331	1340
Dan	M	26-40	7	3677	195	1062
Alexa040200	F	26-40	8	3221	464	484
Zaher020200	M	26-40	8	2746	271	488
Andy R	M	26-40	8	2601	229	816
Thomas	M	26-40	8	4388	393	1692
Edward	M	26-40	9	7108	436	1642
Neil G	M	18-25	9	2786	189	672
Nicola040200	M	26-40	10	5219	360	675
Andy B030200	M	41+	10	3655	306	787
Hugh	M	41+	11	3655	340	1248
Chee	M	26-40	13	6816	208	756
Pieter	M	41+	14	4797	552	1088
Julie	F	18-25	14	6882	347	644
Enric	M	36-40	16	5127	218	494

Table A - Sequence Properties.

The table shows that there is a considerable variety in the number of taps people choose, not obviously dependent of gender or age.

7. RESULTS

Our primary concern during this preliminary investigation was to identify the key characteristics of a pressure sequence. In doing so our aim was a reduction of the raw data sequence to a small manageable key, which we hoped could be used as a unique identifier.

With the key characteristics identified, we would look at the consistency with which people entered their pressure sequence, and make a first attempt at characterising the performance of our system.

7.1. KEY FEATURES OF A PRESSURE SEQUENCE

As a first discriminant in a sequence of pressure pulses we use the number of pulses because it separates participants in the scheme into different sub-groups, making the processing more manageable. However, a rhythm is easily overheard, and copied by an imposter, and we do not rely on this number as a distinguishing feature - see below. The distribution and consistency with which people entered their sequence is shown in Table B.

No.	Name	Modal Pulse No.(MPN)	Samples With MPN	Total Sequences	% Samples With MPN
1	ThomasF090200	2	26	30	87
2	Paul	3	30	30	100
3	Mauricio	3	30	30	100
4	Yavuz	3	30	30	100
5	Marcus030200	3	29	31	94
6	Bob030200	4	30	30	100
7	Dan030200	4	29	33	88
8	Jeff030200	4	30	30	100
9	James030200	4	29	31	94
10	Lesley040200	4	26	35	74
11	Danny030200	5	28	31	90
12	Yalin030200	5	27	30	90
13	Yean030200	6	30	30	100
14	Marijke	6	27	30	90
15	Mark030200	6	27	31	87
16	Peter030200	7	30	30	100
17	Dave030200	7	26	30	87
18	Manabu	7	30	30	100
19	Dan	7	28	30	93
20	Theo040200	7	27	30	90
21	Uli030200	7	28	30	93
22	Zaher020200	8	30	30	100
23	AndyR	8	20	30	67
24	Thomas	8	27	32	84
25	Alexa040200	8	30	30	100
26	Edward	9	22	31	71
27	NeilG	9	23	30	77
28	Andy030200	10	28	31	90
29	Nicola040200	10	27	31	87
30	Hugh	11	29	30	97
31	Chee	12	24	30	80
32	Julie0200	14	26	30	87
33	Pieter	14	26	30	87
34	Enric	16	5	30	17

Table B - Distribution and Consistency of pulses.

Table B shows that approximately 85% of people entered their modal number of pulses, more than 80% of the time. One person in our trial performed particularly badly, entering his most common number of pulses only 17% of the time. We expect that consistency in real word use would be lower than suggested in these controlled measurements, but hopefully not as low as demonstrated by our worst volunteer.

The main features of a pressure sequence are Pulse Height, Pulse Width and Interval Duration. Each pressure sequence of (n) pulses can then be reduced to the form:

Pulse(1)Height, Pulse(1)Width, Interval(1),
Pulse(2)Height, Pulse(2)Width, Interval(2),
...
Pulse(n)Height, Pulse(n)Width.

All recorded sequences were reduced to this form, and an average sequence template generated for each person. Averages from the beginning (ie. First pulse and interval) of each person's template are shown in Table C.

No.	Name	Height (V)	Name	Width (mS)	Name	Interval (mS)
1	Enric	0.36	Pieter	8	Enric	109
2	Thomas	0.37	James030200	9	Neil G	118
3	Edward	0.40	Mark030200	9	James030200	119
4	Julie080200	0.49	Thomas F090200	10	Chee	122
5	Jeff030200	0.5	Nicola040200	11	Andy R	123
6	Theo040200	0.5	Andy B030200	13	Mark030200	142
7	Andy R	0.5	Paul	16	Lesley040200	149
8	Thomas F090200	0.54	Hugh	20	Andy B030200	154
9	Paul	0.56	Mauricio	21	Yean030200	165
10	Nicola040200	0.58	Julie080200	22	Julie080200	180
11	Hugh	0.58	Theo040200	23	Danny030200	182
12	Lesley040200	0.59	Neil G	23	Dave030200	189
13	Yalin030200	0.65	Manabu	23	Yavuz	192
14	Mark030200	0.67	Dan	24	Thomas F090200	194
15	Pieter	0.69	Thomas	24	Theo040200	202
16	Mauricio	0.70	Bob030200	25	Yalin030200	206
17	Uli030200	0.74	Edward	26	Mauricio	212
18	James030200	0.74	Yean030200	27	Edward	224
19	Alexa040200	0.76	Zaher020200	29	Jeff030200	238
20	Dan030200	0.76	Alexa040200	29	Marijke	238
21	Yean030200	0.77	Yalin030200	33	Alexa040200	240
22	Chee	0.77	Jeff030200	33	Zaher020200	244
23	Manabu	0.78	Marcus030200	33	Uli030200	248
24	Marcus030200	0.82	Lesley040200	35	Marcus030200	283
25	Dave030200	0.87	Marijke	36	Pieter	283
26	Andy B030200	0.87	Dan030200	40	Dan	297
27	Peter030200	0.92	Andy R	42	Thomas	306
28	Danny030200	0.93	Uli030200	42	Peter030200	310
29	Neil G	0.94	Peter030200	43	Manabu	314
30	Dan	0.99	Yavuz	45	Bob030200	333
31	Bob030200	1.02	Danny030200	48	Nicola040200	338
32	Marijke	1.09	Chee	50	Hugh	343
33	Zaher020200	1.14	Enric	63	Dan030200	380
34	Yavuz	1.76	Dave030200	85	Paul	445

Table C - Section of Sequence Averages.

Table C (Columns 2 and 3) show the variation in Pulse heights for each person. Height values are given in Volts. The lowest average height is 0.36V, with approximately 68% of this person's Pulse 1 samples falling within the range of 0.23 - 0.51V. The highest First Pulse height average is 1.76V, with 68% of all samples falling between 1.43 and 2.12V. Pulse height exhibits a large variation within our sample and will therefore be considered a useful discriminant.

Columns 4 and 5 show the smallest average first pulse width to be 8mS wide, with 68% of this person's samples falling between 3.7 and 11.3mS. The widest first pulse is 85mS long, with 68% of samples falling between 52 and 118mS.

Columns 6 and 7 show the variation within the first interval. This ranges from the shortest interval being of 109mS duration (with 68% of this person's samples lying between 67.5 and 150.5mS) and the longest interval of 445mS (with 68% of samples falling between 372 and 518mS).

From the tables above it can be concluded that each characteristic; Pulse Height, Pulse Width and Interval duration, all offer a degree of discrimination between sequences. The variation in all characteristics, between samples of different people appears to be smooth. Reliance, therefore, upon one single feature characteristic, will offer only discrimination between characteristics at the extremes of variation. Furthermore, there is little correlation between the relative positions of a person's characteristics within the table. For example Dan is ranked at positions 30,

14 and 26 according to the three characteristics. It should therefore be concluded, that a combination of all three characteristics would provide greater discrimination potential.

With the key characteristics; number of pulses, pulse height, pulse width and interval duration identified, the next section describes typical performance of an identification system using pressure sequences.

7.2. FALSE REJECTION RATES

As mentioned above, all sequences collected from each person have been combined into an average sequence for that person. This will be used as an identifier template for that person. In this section all sequences gathered from a person will be compared to their average sequence, under a range of acceptance tolerances. The number of legitimate sequences rejected, expressed as a percentage of number of tries, is known as the False Rejection Rate (FRR).

The method of comparison was as follows:

1 The number of features is: (pulse height, pulse width interval) × number of pulses. This ranges from 3×2 to 3×14 features.

2 For each of the 34 volunteers:

For each percentage between 0 and 100:

(a) Set the acceptance range to the feature set as the average +/- the percentage

(b) For each of the sequences of pulses of the current volunteer (the majority have tapped 30 sequences):

i Calculate for how many of the sequences the entire feature set is within the acceptance range. This gives the number of false rejects on the basis of the range alone.

ii Since some of the sequences do not have all the required features, they are rejected as well. Add this to the number of false rejects on the basis of the range alone, giving a total number of false rejects.

Figure 2 shows the FRR (and FAR) for one of the volunteers plotted against percentage tolerance. Below a tolerance of 8%, all legitimate sequences are rejected; between 8 and 14% FRR decreases rapidly, until, 15% and above, where all legitimate sequences are accepted. The characteristics of FRR curves from all other volunteers are similar, with FRR dropping to a minimum after 9% (Andy R) to 72% (Pieter) tolerance.

7.3. FALSE ACCEPTANCE RATES

The False Acceptance Rate (FAR) describes the proportion of impostor sequences, which are falsely accepted to be another's sequence. The method of calculation is similar to that outlined above, the key difference being that all sequences from other people are compared to the template sequence of one person. The acceptance threshold is varied, as above. Each impostor sequence which has both the correct number of pulses and which passes the threshold comparison is deemed a false acceptance. A typical FAR curve is shown Figure 2. The curve labelled

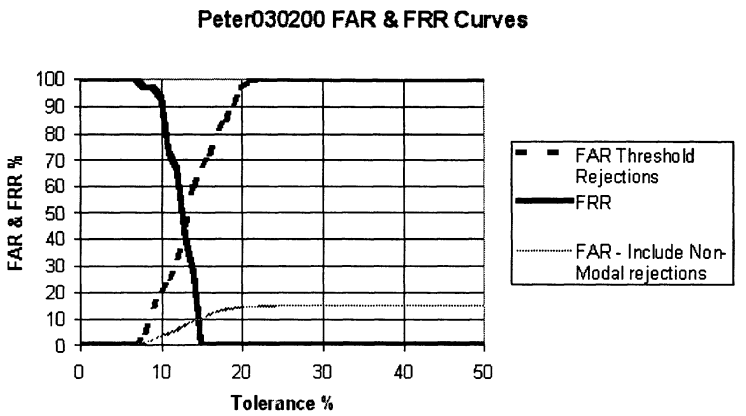

Figure 2 Typical FAR and FRR Curves

'FAR - Threshold Rejections' considers only those sequences with the same number of pulses as the template. The number of pulses in a sample is a discontinuous variable and is a function of the consistancy with which people enter their sequences. If sequences with a non-modal number of pulses is included in the FAR calculation, then the resulting FAR will be artificially low. The 'Threshold Rejections' curve was generated by the comparison of Peter030200's reference template with all other sequences of seven pulses.

Again this shows an increased FAR beyond a tolerance of 8%. Beyond 20% almost all other sequences are accepted.

The curve, labelled 'FAR - Include Non-Modal Rejections', is the result of comparing Peter030200's reference template with all other samples, irrespective of their number of pulses. All sequences not containing seven

pulses were immediately rejected. To further quantify the discrimination amongst our entire sample, it was found that approximately 15% of all sequences contain seven pulses.

Since it is relatively straightforward for the number of pulses entered by a legitimate user, to be either overheard by a third party or systematically guessed, we believe that the higher FAR curve is more appropriate.

7.4. EQUAL ERROR RATES

The Equal Error Rate (EER) is the point at which FAR equals that of FRR. EER gives some indication of a biometric scheme's performance, and is inversely proportional to discrimination. Table D shows the EER for each of our volunteers.

Volunteer	EER %	Tolerance at crossover
Pieter	100	54.5
Thomas	95.3	38.3
Yavuz	94.6	33
Manabu	93.9	25.7
Mark030200	90.4	47.1
Bob030200	80.7	19.8
Edward	80	24.3
Danny030200	79.8	14.8
Nicola040200	74	27.9
Thomas 090200	66.8	23.3
Dan	62.2	22.7
Marijke	57	16.1
Dan030200	55.9	17.7
Marcus030200	55	25
Paul	48	27.5
Hugh	46.3	24
Peter030200	46.1	12.5
Uli030200	44.4	13.1
Dave030200	43.9	12.4
Mauricio	42.8	24.6
Zaher020200	41	14.1
Theo040200	39.4	31.1
Lesley040200	32.9	15.2
James030200	27	21.8
Yalin030200	26	13.9
Alexa040200	23.6	12.6
Andy R	23	8.8
Yean030200	19	14.2
Chee	15	10.7
Jeff030200	14	14.7
Neil G	3	18.8
Andy B030200	0	25
Julie080200	0	15
Enric	0	20

Table D - Equal Error Rates

From our data it can be seen that the Equal Error Rates are high. This is not necessarily a problem; by reducing threshold tolerance, the number of false acceptances will fall, and our system's chance of correctly verifying identity will improve. The drawback in doing so is an increase in the rate of false rejections.

The Equal error rates range from 0 to 100, in our volunteer's sequences. Low equal error rates, predominantly occurring in sequences with large numbers of pulses, arise from the limited number of other sequences with comparable pulse numbers. It is expected that EER values for such sequences will rise as more sequences are captured. A high value of EER arises from the variation with which people entered their chosen sequence.

From our data, only one volunteer (Pieter) could not be unambiguously identified. Again, as samples from more people are collected, we would expect this number to rise.

8. CONCLUSIONS AND FURTHER WORK

Based on the simple idea that you can tell who is knocking on your door by the sound alone, we have devised a method to verify the identity of a user to a smart card. An inexpensive, screen-printed piezoelectric pressure sensor is integrated on a smart card. The signals are measured and matched to the templates of a group of volunteers. With a simple matching algorithm we are able to identify all but one of our 34 volunteers. The EER is high but we have barely scratched the surface of what is possible with our apparatus.

It is commonly accepted that the performance of biometric systems steadily improves as the subjects learn to give consistent measurements [7]. Our experiment collected a unique set of sequences, from each volunteer. They were given no immediate response on the quality of their measurements, and were, thus, unable to demonstrate improvement. This is an area for future work.

Further, our reference templates were crudely constructed - we used all sequences from a person, containing their modal number of pulses. Rather than taking a blind average of these sequences, we propose discarding any statistical outliers before creating reference templates.

We have performed simple analysis upon a simplified representation of our data. Even so, the results show that there are measurable differences in the sequences tapped out by each person. We looked at the absolute duration of pulses and intervals, rather than the relationship between each feature. Since, rhythms have tempo, and tempos can be changed whilst retaining the rhythm's overall structure, we aim to use both geometric and time-invariant tools to discover any underlying structure to the sequences.

Our next step is to investigate whether there exist measurable differences in the 'tap' itself. We will look at both the bio-mechanics of tapping (to theoretically assess possible discrimination), and at the detailed data already collected using more powerful analysis and matching techniques, such as hidden Markov Models, and Neural nets [1].

To integrate the measurement circuitry with the other components of a smart card we envisage a similar approach as that used to build dual interface cards [3]. These combine RF rectifier, receiver and transmitter with regular smart/memory card circuitry. The antenna is connected to the circuit as part of the packaging process. Using the same process we

expect to be able to integrate our charge amplifier, and ADC on the chip, with the remaining smart card circuitry. It would also interesting to investigate how one could exploit the capabilities of current dual-mode smart cards by replacing the antenna by a suitable (capacitive or resistive), screen printed sensor.

It is easy for an eavesdropper to overhear a sequence of knocks, to memorise it and to use the same sequence on a stolen card. Therefore, we plan to experiment with a sequence of squeezes, which would be noiseless. The current detector is sensitive enough to measure gentle squeezes and the dynamic range of the sensor and electronics is adequate.

Our group of volunteers is just large enough to draw statistically meaningful conclusions. However, we should like to conduct an experiment, with a larger randomly selected group of volunteers that is representative for the population at large.

The pressure sequence system offers smart cards the ability to verify the identity of its user without having to rely on external devices (except for power and clock). This is a valuable property because external devices could be tampered with. The smart card can thus be confident of user proximity. Tampering with the sensor on the smartcard itself is always possible. Counter measures would include monitoring electrical properties of the detector, such as its capacitance, resistance and impedance. This is an area of further work.

Acknowledgements

We thank Eduard de Jong, Thomas Papakostas and Neil White for their help and comments, and we thank our volunteers for participating in the experiment. Oberthur has donated the smart cards for our experiment.

References

[1] T. J. Alexandre. Biometrics on Smartcards: An Approach to Keyboard Behavioral Signature Future Generation Computer System. 13(1):19-26, Jul. 1997.

[2] R. J Anderson. Why Crypto systems fail. Communications ACM 37(11):32-40, Nov. 1994

[3] F. Christian. From RFID to the dual circuit - contact and contactless smart card circuit on the same IC. Smart Card 1997 convention proceedings, pp 69-77, Quality Marketing Services Ltd, Peterborough.

[4] K. Gilleo. Polymer Thick Film. Van Nostrand Reinhold, New York, 1996

[5] H. Grun. Optimised smart card materials and environmental impact. Smart Card 1997 convention proceedings, pp 69-77, Quality Marketing Services Ltd, Peterborough, UK.

[6] K. Hyun-Jung. Biometrics, Is it a viable proposition for identity authentication and access control? Computers and Security, 1998, 14(3), pp 205-215

[7] A. Jain, R. Bolle & S. Pankanti (Editors). Biometrics: Personal Identification in Networked Society. Kluwer/Boston, 1998

[8] A. Jain, L. Hong & S. Pankanti. Biometric identification. Communications of the ACM 43(2):90-98, Feb. 2000

[9] R. Joyce & G. Gupta. Identity Authentication based on keystroke latencies. Communications ACM 33(2):168-176, Feb. 1990.

[10] E. Kandel & J. Schwartz. Principles of Neural Science. Elsevier/North-Holland, New York, 1981.

[11] M. Lapere & E. Johnson. User authentication in mobile telecommunication environments using voice biometrics and smartcards. Lecture Notes in Computer Science, V1238 1997, pp 437-443

[12] B. Miller. Vital Signs of Identity. IEEE Spectrum, February 1994, pp 22-30

[13] F. Monrose & A. Rubin. Authentication via keystroke dynamics. 4th ACM Conference on Computer and Communcations Security (April, 1997).

[14] T. Papakostas & N.M. White. Polymer Thick-Film Sensors and Applications, in Sensors and their Applications X, Cardiff, UK, pp 125-130

[15] J.R. Parks. Personal Identification - Biometrics, Information Security. pp 181-191, Elsevier Science/North Holland 1991

[16] N. M. White & J. D. Turner. Thick-film sensors: past, present and future. Measurement Science and Technology V8, 1997 pp 1-20

[17] D. Wilson. Smarter Solutions for Smartcards. Computer Design, February 1997, pp 34-36