Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed
Computing

Signature Detection in Mobile Payments

Master Thesis

Cedric Waldburger

wcedric@ee.ethz.ch

Distributed Computing Group
Computer Engineering and Networks Laboratory
ETH Zürich

Supervisors:
Christian Decker (DISCO)
Conor Wogan (SumUp)
Prof. Dr. Roger Wattenhofer

January 11, 2013

Acknowledgements

thank DISCO/Christian/Prof

thank SumUp

thank Thomas Stämpfli / Tobias Ruland / SignatureNet / ...

Abstract

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Keywords: Keywords go here.

CR Categories: ACM categories go here.

Contents

Chapter 1

Introduction

Rough draft:

Mobile Payments are interesting because blablabla...

Problem: How to make them secure? Chip & Pin (most secure) is not in production yet and is expensive. So: Chip&Signature - but how to make it secure? Mag Stripe is easiest to create but also easiest to do Fraud/Attack

Copied:

Smartphones and notebooks are becoming increasingly popular. These devices hold privacy critical information such as contact lists, email account access, web- browser passwords, communication history with contacts and so on. Additionally these devices are mobile and hence exposed to a higher risk of being accessed by unauthorized users. Therefore it seems necessary to explore new ways to protect this data using existing hardware. In the notebook industry, fingerprint readers and file encryption are becoming increasingly popular. Modern mobile phones provide lockscreens, which require a user to enter a code or draw a simple pat- tern on the touchscreen. These authorization mechanisms help to protect critical data more or less effectively. Fingerprint readers can be considered to be fairly secure, whereas current lockscreens are rather easily bypassed. A code or pattern entered on a touchscreen device can be observed either directly or by looking at the smears left by the finger on the screen. The simplicity of the entered token allows an adversary to easily observe and reproduce it. Compared to the finger- print reader, a lockscreen code or pattern contains very little information which can easily be stolen. Because acquiring a fingerprint requires special hardware, this thesis is focused on exploiting a users signature as the basic authentication token.

The proliferation of touchscreen-enabled devices represents many new promising scenarios and applications for signature verification. Automatic signature verification is a challenging task per se, as it must face a notable variability among signatures from the same individual and the risk of highly skilled forgers which, due to their unpredictable nature, are not completely possible to model during the design of a verification system. This work is focused on automatic person authentication using signature as a biometric trait. Dynamic signature verification for portable devices is studied and an analysis of its specificities compared to traditional signature verification systems based on digitizing tablets is performed. Within biometrics, signature is one of the most socially accepted biometric traits, as it has been used in financial and legal transactions for centuries (Fierrez and Ortega-Garcia, 2007b; Plamondon and Lorette, 1989). In the current era of electronic services and ubiquitous access to information, secure access control and user authentication are common tasks which are usually performed with tokens or passwords. In this field, biometrics has become a focus of interest as it uses anatomical (e.g. fingerprint, iris) or behavioral (e.g. voice, signature) traits to authenticate a user (Jain et al., 2004). These traits cannot be easily stolen or forgotten. It is now common to observe fingerprint verification systems in portable electronic devices (e.g. handhelds), face recognition systems for border control purposes and iris verification in some airports (e.g. United Arab Emirates). Biometric authentication has gathered an increasing research and commercial interest in the last few years (Jain et al., 2006) as it represents a convenient and secure means of person authentication.

1.1 SumUp Mobile Payments

1.1.1 Business Model

Traditional Terminals: High initial cost, high monthly fees, high minimum transaction limits

=¿ Solution: Use merchant's mobile devices (iOS, Android) to collect accept credit cards

=¿ Collect fixed percentage per transaction

on the technical side: multiple operation modes - online transaction (ecom), ... depending on the hardware used

1.1.2 Facts & Numbers

- list countries where sumup is active

- many thousand merchants to date

1.2 Fraud

As with every payment system, fraud plays a role

most common fraud cases: ...

and link them to the technology used (mag stripe, chip & signature, ...)

1.3 Signature Recognition

How to approach that without the complicated and expensive chip&pin device?

Use signature detection to determine if someone is who he/she claims to be

Chapter 2
Fraud

2.1 Fraud Scenarios

2.2 Fraud Detection

2.3 Fraud Prevention

Chapter 3

Signature Recognition

An offline signature verification method can classify a static image of a signature whereas an online signature verification method also con- siders the dynamics of the signing process.

3.1 Related Work

SVC2004 Dataset -

3.2 Online Signature Detection

Online signature verification methods are generally categorized to either use global or local features to classify a given signature

==

On-line or dynamic systems use captured signature time-functions. These functions are obtained using digitizer tablets or touchscreens (e.g. Tablet-PCs, smart phones, etc.). Tradition- ally, dynamic systems have presented a better performance than off-line systems as more levels of information than the signature static image are available (Plamondon and Lorette, 1989). This is the approach considered in this work, and will be described in the following chapters.

Feature Extraction: Two main approaches have been followed in this step: feature- based systems extract global features (e.g. signature duration, number of pen-ups, average velocity) from the signature in order to obtain a holistic feature vector (Lee et al., 1996). On the other hand, function-based systems use the signature time functions (e.g. position, pressure) for verification. Traditionally, function-based approaches have yielded better results than feature-based ones (Fierrez-Aguilar et al., 2005a; Kholmatov and Yanikoglu, 2005).

3.2.1 Feature-Based Methods

As the name suggests, feature-based methods use features extracted from the sig- natures to perform the verification task. In general two different types of features are considered: global and local. Global features are related to the signature as a whole, for instance the signature duration or the mean pressure applied. Local features are based on single sample points. Examples for local features are the maximum velocity or the highest curvature.

Lee et al. [5].

A large number of features useful for signature verification was listed by Fierrez-Aguilar et al. [6].

This is why in general a smaller set of more discriminative features is preferred. The issue of feature selection in the signature verification task was extensively studied by Richiardi et al. [7].

After having found a suitable feature vector, an arbitrary one-class classification scheme can be used to perform the classification into valid and invalid signatures. Since there is no negative training data available, the task of classification is very similar to the task of outlier- or novelty detection. Several methods to perform such a classification are known [8].

3.2.2 Function-Based Methods

Function-based signature verification methods are focused on building a signature model which accurately reflects the temporal behaviour of the signature. Instead of extracting features that are used for verification, the emphasis of the signature model lies in the (timed) sequence of strokes drawn during the signing process. Comparing any signature to the model built during training will lead to a match score which is based on the level of similarity between (timed) sequence of strokes in the model and the signature under test. Function-based methods are reported to deliver better performance than global feature based methods [6]. Two function-based methods are predominant in the literature: Hidden Markov Model based methods and Dynamic Time Warping (DTW) based methods.

page 6-8 for sample feature set

Function-based methods to perform signature verification compare the temporal behaviour of the recorded signals x(t), y(t), p(t) and a(t). In this work, a dynamic time warping based method is used. The performance of a Hidden Markov Model system might be higher than the DTW system performance but the implementation complexity is much lower for the DTW system.

DTW - Dynamic Time Warping

Dynamic time warping is a classic dynamic programming algorithm that is also used in speech recognition.

A signature verification system using DTW is reported by Martens and Claesen [14]. DTW is a method to measure the similarity between two sequences which may vary in time or speed. This similarity measure can be used to perform signature verification. Comparing two sequences can be done in many different ways such as correlation, integration of the difference of two signals etc. However all these similarity measures cannot cope with non-linear time distortions which we will have in the signature signals. If a user takes a little longer for the first letter of the signature, the similarity measure should not deteriorate more than if the user was taking a little longer on the last letter. The DTW method allows us to compare two signatures while a small time distortion in the beginning of the signature does not accumulatively deteriorate the similarity measure throughout the whole signature.

page 10-12

DTW Signature Verification

Training the DTW signature verification algorithm is performed by calculating the distance measure (dtw[n][m]) for all pairs of signatures in the training set. The signature with the smallest mean distance measure to all the other signatures is selected as the prototypical signature of the given user. The DTW matching score of a signature to be verified is equal to the distance measure dtw[n][m] between the prototypical signature found during training and the signature under test.

== Although the DTW algorithm has been replaced by more powerful ones such as HMMs or SVMs for speech applications, it remains as a highly effective

Hidden Markov Model

Hidden Markov Models (HMM) have been widely used by the speech recognition community (Ra- biner, 1989) as well as in many handwriting recognition applications (Dolfing, 1998). Sev- eral approaches using HMMs for dynamic signature verification have been proposed in the last years (Dolfing et al., 1998; Fierrez et al., 2007; Muramatsu and Matsumoto, 2003; Van et al., 2007; Yang et al., 1995). An HMM represents a double stochastic process, governed by an underlying Markov chain, with a finite number of states and random function set that gen- erate symbols or observations each of which is associated with one state (Yang et al., 1995). Observations are modeled with GMMs in most speech and handwriting recognition applica- tions. GMMs, which can be considered a single-state HMM, have been also successfully used for signature verification

(Richiardi and Drygajlo, 2003).

more: p13++ Martinez08

Finding a reliable and robust model structure for dynamic signature verification is not a trivial task. While too simple HMMs may not allow to model properly the user signatures, too complex models may not be able to model future realizations due to overfitting. On the other hand, as simple models have less parameters to be estimated, their estimation may be more robust than for complex models.

3.3 Offline Signature Detection

3.4 Challenges in Signature Detection in Mobile Payments/at SumUp

3.4.1 Signature written with Finger vs Pen

3.4.2 Sparse Initial Dataset

3.4.3 Device & Software Fragmentation

Chapter 4

Experiments

4.1 Databases

most available signature DB are pen/tablet signatures

4.1.1 SumUp

4.1.2 SVC2004

Two development databases were released prior to the Signature Ver- ification Competition (SVC) 2004 (Yeung et al., 2004). They were captured using a WACOM digitizing tablet and a Grip Pen. Due to privacy issues, users were advised to use invented signatures as genuine ones. The two databases differ in the available data, and correspond to the two tasks defined in the competition. One contains only coordinate information while the other provides also pressure and pen orientation signals. Each database contains 40 users, with 20 genuine signatures and 20 forgeries per user acquired in two sessions. Both occidental and asian signatures are present in the databases. Examples of signatures from this database are shown in Fig. 2.6.

4.1.3 SUSig

4.1.4 ATVS-SSig_DB

4.2 Experimental Setup

4.3 Feature Selection

== Due to the curse of dimensionality (Theodoridis and Koutroumbas, 2006), the performance of a statistical classifier is degraded if the available training data is too small compared to the number of dimensions of the feature vector (Jain and Zongker, 1997). This is usually the case in signature verification, where the average length of a digitized signature is of a few hundreds of samples and the available number of training signatures is relatively small (in practical applications between 3 and 5). The amount of training signatures is mostly conditioned by the willingness of the users to provide many samples during enrollment. Nevertheless, when signatures are captured during only one unique session, their variability is small in general, leading to a poorly trained model. Feature selection techniques try to reduce the dimensionality of the feature vectors while optimizing the verification accuracy. Their goal is to find the optimum combination of features according to a given optimization criterion. Ideally, given a feature vector of F dimensions, all the possible combinations from 1 to F features should be tested in order to find the optimal combination. p15++

4.4 Results

4.4.1 Signature Detection

4.4.2 Feedback Loop

Chapter 5

Conclusions

Chapter 6

This is the first chapter

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua.

6.1 This is the first section

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua.

6.1.1 And this the first subsection

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua.

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Figure 6.1: Example figure.

Header 1	Header 2	Header 3	Header 4
Row 1	15	17	12
Row 2	13	1	8

Table 6.1: Example table.

And here we reference our only figure 6.1 and table 6.1.

Theorem 6.1 (First Theorem) *This is our first theorem.* ◇

PROOF And this is the proof of the first theorem with a complicated formula and a reference to Theorem 6.1. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua.

$$\frac{\mathrm{d}}{\mathrm{d}x}\arctan(\sin(x^2)) = -2 \cdot \frac{\cos(x^2)x}{-2+(\cos(x^2))^2} \tag{6.1}$$

Here a reference to the above equation (6.1). ■

And lastly, we cite an external document [1]. And lastly, we cite an external document [2]. And lastly, we cite an external document [3].

Bibliography

[1] One, A., Two, A.: A theoretical work on computer science. In: 30th Symposium on Comparative Irrelevance, Somewhere, Some Country. (June 1999)

[2] Bissig, P.: Dynamic signature verification for portable devices. Master's thesis, ETH Zurich

[3] Diaz, M.M.: Dynamic signature verification for portable devices. Master's thesis, Universidad Autonoma De Madrid

Appendix A

Appendix Chapter