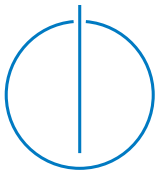
DEPARTMENT OF INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Bachelor's Thesis in Informatics

Pattern Recognition with Smart Devices as Personal Authentication Factor

Philipp Fent



DEPARTMENT OF INFORMATICS

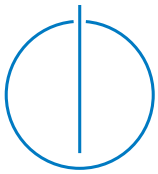
TECHNISCHE UNIVERSITÄT MÜNCHEN

Bachelor's Thesis in Informatics

Pattern Recognition with Smart Devices as Personal Authentication Factor

Mustererkennung mit Mobilgeräten als persönliches Identifikationsmerkmal

Author:	Philipp Fent
Supervisor:	Prof. Dr. Uwe Baumgarten
Advisor:	Nils T. Kannengießer, M.Sc, Prof. Senjun Song, Ph.D.
Submission Date:	15. February 2016



I confirm that this bachelor's thesis in informatics is my own work and I have documented all sources and material used.

Munich, 15. February 2016 Philipp Fent

Acknowledgments

TODO: Acknowledgments

Abstract

Every person displays characteristic patterns of behavior, that can be used to verify her or his identity. With the rise of personal smart devices, e.g. smartwatches or smartphones, these patterns can be recorded and analyzed.The resulting characteristics can be used as an additional factor in Multi–Factor Authentication or used as an intrusion detection system by reporting anomalies. In this paper, we analyze the patterns for motion, determined by measuring acceleration. We then evaluate how to efficiently, accurately, and practically extract behavioral patterns, identifying individual users. Furthermore, we developed Android smartphone and smartwatch app prototypes demonstrating the identification capabilities.

TODO: conclusion

Menschen besitzen charakteristische Verhaltensmuster, durch die sie eindeutig identifiziert werden können. Durch ständig mitgeführte Mobilgeräte, z.B. Smartphones oder Smartwatches, können diese Muster aufgezeichnet und analysiert werden. Die daraus abgeleiteten Merkmale können als zusätzlicher Faktor bei Multi-Faktor-Authentifizierungsverfahren oder als Angriffserkennungssystem eingesetzt werden. Im Rahmen dieser Arbeit werden diese Muster anhand von Beschleunigungssensoren, hinsichtlich effizienter und präziser Verhaltensmustererkennung, analysiert. Dies wird durch einen Prototypen einer Android Smartphone und Smartwatch App demonstriert.

Contents

1 Introduction

Modern computer systems are facing TODO. Users are one of the most commonly exploited things around computers, especially in social engineering and fishing. Most systems currently rely on a standard combination between username and password. Already in 2009, Aloul et al. described the most common security concerns with passwords:[AZE09] “Users tend to use easy-to-guess passwords, use the same password in multiple accounts, write the passwords or store them on their machines, etc. Furthermore, hackers have the option of using many techniques to steal passwords such as shoulder surfing, snooping, sniffing, guessing, etc.”

Furthermore, many users tend to stay logged into services with their mobile devices (TODO: Statistiken?), despite not having appropriate security measures for their devices. On most Android phones, full disk encryption is not enabled by default, which leads to another attack vector for identity theft.

Aloul et al. introduced a system of One Time Passwords (OTPs) using mobile phones, which significantly improves security by introducing a second factor of authentication. However, for authentication situations on smartphones themselves the OTP mechanism is rendered pretty much useless, as the second factor is in fact on the same device. [Bis06]

1.1 Vision

The whole vision of this thesis, is to provide a way to easily detect individual users by a short authentication sequence based on acceleration patterns. Even though this does not qualify as cryptographically secure authentication, behavioural patterns and keystroke recognition can be used as biometric authentication aids. For example, Bhargav-Spantzel et. al.[BSB06] described a system to extract cryptographic biometric keys from biometric data and how this can be combined with additional other proofs of identity to provide strong authentication.

With acceleration pattern recognition, we will make a authentication mechanism

with zero additional user interaction possible. This allows for higher frequency user re–authentication without disturbing and annoying the user. That means, instead of prompting the user with a login screen every 24 hours, we can measure his or her acceleration patterns every time sensitive information is accessed. Therefore, we can not only provide basic login authentication, but also provide a way for users to stay authenticated for longer sessions or even detect when someone else hijacks a valid session. Since the time between two authentication requests can almost be arbitrarily small, an attacker who gets control over the current session will get a new authentication request relatively quickly, thus minimizing the potential damage.

1.2 Single user licenses

Another application of this technique is to identify individual users, even if using the same device. This might not only be useful in terms of individualizing the software according to the current user, but also for tracking of software usage.

A common licensing model for software are per–user licenses, i.e. n licenses for n users of the software. However, this license model currently cannot be enforced, since the software is installed on a single physical device, which may be shared among users. This led to most software companies licensing their software per–installation instead of per–user. As of 2016, many users tend to have multiple devices and also want to use their licenses on multiple devices. This resulted in a trend to bind software licenses to user accounts instead of devices. This trend is also prevailing in modern Software as a service (SaaS) models, which do not require installation of the software on end–user devices anymore. A possible circumvention of these account bound licenses is account sharing. This imposes a real problem, not only for software licensors, but also for other access providers. For example a consumer research from Parks Associates[Par] reports, that “6% [of video streaming users] are exclusively using shared accounts to access subscription”.

The methods described in this theses can give a powerful way to detect individual users sharing physical devices, as well as sharing individual accounts and thus reduce copyright infringements that could not even be detected beforehand.

1.3 Multi–factor authentication

Multi–factor authentication (MFA) is a technique to enhance security in access control situations. It combines multiple forms of authentication mechanisms, based on conceptually different approaches: Knowledge, e.g. passwords or PINs; possessions, e.g. keys or bank cards and biometric characteristics, like fingerprints or, as in our approach, behavioural patterns.

A typical authentication attempt with MFA is only successful, when all needed factors are present. The most common example for MFA is banking, where one needs to be in possession of the banking card and needs to know the card's PIN. However, an attack vector targeting this system is copying the banking card while the attacked person does not notice his card being copied. This attack vector is also possible with biometric characteristics and even relatively easy, as many biometric traits are publicly visible. Fingerprints have proven to be copyable with low cost[es08] and new high resolution cameras allow to photograph fingerprints and eyes in high enough quality to spoof many scanners[FKH14]. These attacks also can be adapted to other authentication systems based on visible biometric traits, such as iris recognition or Android's Face Unlock.

For biometric authentication to be sufficiently secure, the traits need to be intrinsic, i.e. not publicly visible, and hard to copy. Acceleration based motion detection matches these requirements, as recording of these patterns is only possible with physical access to the authentication device or very close monitoring of all body movement of the user.

1.4 Smart mobile devices

Smart devices are electronic devices, that feature wireless communication, e.g. WiFi or Bluetooth. Smart *mobile* devices are smart devices, that are typically worn or kept in close proximity to the user. This usage usually results in small form factors and little weight. These devices are most often commodity devices and used frequently. Therefore, smart mobile devices are ideal to provide authentication, since the authenticating user is accustomed using the device.

Common examples for smart mobile devices are smartphones and smartwatches.

TODO: Füllbild?

1.4.1 Smartphones

Smartphones are the most capable of the smart mobile devices discussed herein. Smartphones usually have numerous wireless communication possibilities and thus function are a personal data–hub, to which other personal devices connect and communicate over.

1.4.2 Smartwatches

1.4.3 Smart–rings

1.5 Pattern recognition

TODO: hier schaubild einfügen

1.5.1 Preprocessing

1.5.2 Feature extraction

Dynamic time warping

1.5.3 Classification

Support Vector Machine
k-Nearest Neighbor
Bayes classifier
Neuronal networks
Machine learning with encog
Tensorflow

2 Approaches

2.1 Key stroke recognition

2.1.1 Related work

2.1.2 Identification of taps

Peak detection algorithm [Pal+09]

2.1.3 Features of keystrokes

[DC13] Possible measurements for "keytrokes":
Speed
Intensity
Hold duration
Timespan between taps
"Flight and dwell time"

2.1.4 Adaption to phones

2.1.5 Adaption to watches and keyboards

MotionLeaks discussed on MobiCom'15

2.2 Gait recognition

2.2.1 Related work

2.2.2 Device limitations

2.2.3 Classification

3 Implementation

3.1 Platform identification: Device vs. Server

Privacy aspects with zero-knowledge [BSB06]

3.2 General purpose Android acceleration pattern detection library

3.2.1 Sensor measurement framework

3.2.2 Feature extraction from SensorData

3.2.3 Classification and machine learning

3.3 Data storage and processing

3.3.1 SQLite Database

3.3.2 Background verification of patterns

3.4 App prototypes

3.4.1 Android phone application

3.4.2 Android Wear application

3.4.3 Limitations

4 Evaluation and Interpretation

4.1 Test setup

4.2 Rejection rate vs. accuracy tradeoff

4.3

5 Conclusion

5.1 Current state

5.2 Future prospects

Glossary

computer is a machine that. . . .

Acronyms

MFA Multi–factor authentication.

OTP One Time Password.

SaaS Software as a service.

TUM Technische Universität München.

List of Figures

List of Tables

Bibliography

[AZE09] F. Aloul, S. Zahidi, and W. El-Hajj. “Two factor authentication using mobile phones.” In: *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on*. IEEE. 2009, pp. 641–644. URL: http://staff.aub.edu.lb/~we07/Publications/Two%20Factor%20Authentication%20Using%20Mobile%20Phones.pdf.

[Bar97] D. Bartmann. “PSYLOCK—Identifikation eines Tastaturbenutzers durch Analyse des Tippverhaltens.” In: *Informatik'97 Informatik als Innovationsmotor*. Springer, 1997, pp. 327–334.

[Bis06] C. M. Bishop. *Pattern recognition and machine learning*. springer, 2006.

[Bra] T. Braun. *User authentication from acceleration sensor data*. http://www.mobsec.rub.de/media/mobsec/arbeiten/2014/12/12/2014-ba-braun-knockknock.pdf. Accessed: 2015-12-10.

[BSB06] A. Bhargav-Spantzel, A. Squicciarini, and E. Bertino. “Privacy preserving multi-factor authentication with biometrics.” In: *Proceedings of the second ACM workshop on Digital identity management*. ACM. 2006, pp. 63–72.

[CF07] N. L. Clarke and S. Furnell. “Authenticating mobile phone users using keystroke analysis.” In: *International Journal of Information Security* 6.1 (2007), pp. 1–14.

[DC13] P. R. Dholi and K. Chaudhari. “Typing pattern recognition using keystroke dynamics.” In: *Mobile Communication and Power Engineering*. Springer, 2013, pp. 275–280.

[es08] evelyn and starbug. “Basteltips Biometrieversand.” In: *die datenschleuder* 92 (2008), 56f.

[FKH14] T. Fiebig, J. Krissler, and R. Hänsch. “Security impact of high resolution smartphone cameras.” In: USENIX Association, 2014.

[JW] A. H. Johnston and G. M. Weiss. *Smartwatch-Based Biometric Gait Recognition*. http://storm.cis.fordham.edu/gweiss/papers/btas-2015.pdf. Accessed: 2015-12-10.

[Män+05] J. Mäntyjärvi, M. Lindholm, E. Vildjiounaite, S.-M. Mäkelä, and H. Ailisto. "Identifying users of portable devices from gait pattern with accelerometers." In: *Acoustics, Speech, and Signal Processing, 2005. Proceedings.(ICASSP'05). IEEE International Conference on*. Vol. 2. IEEE. 2005, pp. ii–973.

[Mil+12] E. Miluzzo, A. Varshavsky, S. Balakrishnan, and R. R. Choudhury. "Tapprints: your finger taps have fingerprints." In: *Proceedings of the 10th international conference on Mobile systems, applications, and services*. ACM. 2012, pp. 323–336.

[Mos+09] R. Moskovitch, C. Feher, A. Messerman, N. Kirschnick, T. Mustafić, A. Camtepe, B. Löhlein, U. Heister, S. Möller, L. Rokach, et al. "Identity theft, computers and behavioral biometrics." In: *Intelligence and Security Informatics, 2009. ISI'09. IEEE International Conference on*. IEEE. 2009, pp. 155–160.

[Pal+09] G. Palshikar et al. "Simple algorithms for peak detection in time-series." In: *Proc. 1st Int. Conf. Advanced Data Analysis, Business Analytics and Intelligence*. 2009.

[Par] Parks Associates. *Nearly 60% of U.S. broadband households use OTT video services, but "Account Sharing" is prevalent*. `http://www.parksassociates.com/blog/article/cus-2015-pr11`. Accessed: 2015-12-10.

[SR07] A. P. Shanker and A. Rajagopalan. "Off-line signature verification using DTW." In: *Pattern recognition letters* 28.12 (2007), pp. 1407–1414.

[WLR15] H. Wang, T. T.-T. Lai, and R. Roy Choudhury. "MoLe: Motion Leaks through Smartwatch Sensors." In: *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. ACM. 2015, pp. 155–166.