



Embedded Interactive Systems Laboratory

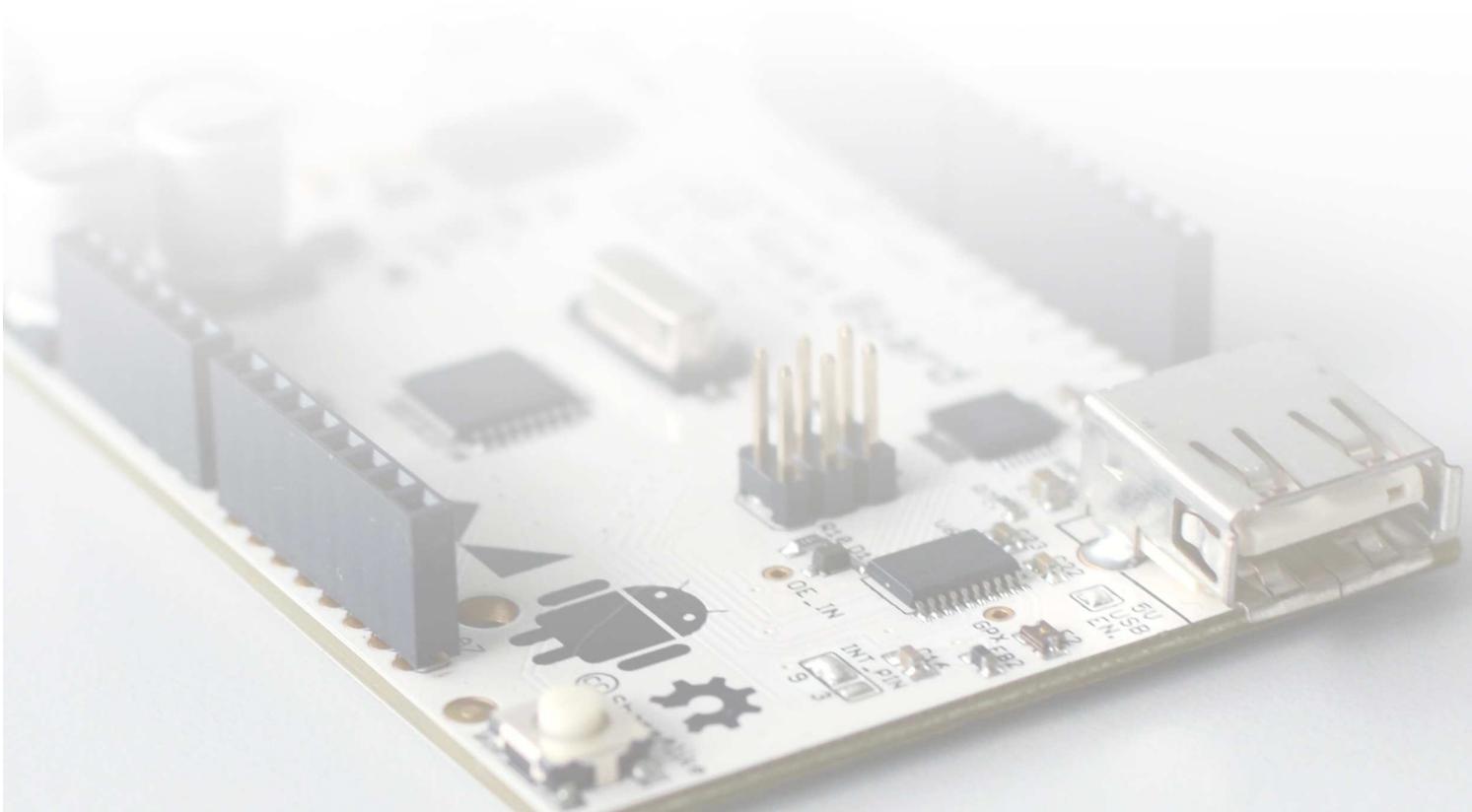


Tobias Stockinger, Patrick Lindemann, Marion Koelle, and Matthias Kranz (Editors)

Fun, Secure, Embedded

Advances in Embedded Interactive Systems
Technical Report – Summer 2014

Volume 2, Issue 3. ISSN: 2198-9494



Fun, Secure, Embedded

Patrick Lindemann, Tobias Stockinger, Marion Koelle, and Matthias Kranz

October 2014

Contents

Preface	4
Gamification of the Quantified Self <i>Stefan Bildl</i>	5
Präventionstechniken gegen Phishing <i>Anna Eiberger</i>	10
Crowdsourcing with Gamification <i>Fabian Göttl</i>	15
Usable Security <i>Jakob Kasbauer</i>	20
Challenges in Crowd Monitoring <i>Aaron Kopp</i>	26
Encryption in the Internet of Things <i>Florian Kovacs</i>	31
Mit Gamification zum Eco-Driving: die Zukunft vor den Augen oder doch im Ohr? <i>Magdalena Murr</i>	35
Alternativen zu Passwort und PIN <i>Maximilian Steindl</i>	40
Wearable Computing: Smart Watches <i>Sebastian Witt</i>	45
Copyright Notes	50

Preface

Embedded systems pervade our daily lives and one can only assume the reasons for this rapid growth of everyday technology. Part of it can be attributed to the frequently inherent excitement and fun that new gadgets bring about. However, we believe that the arising privacy and security issues should be just as prioritized as the user experience. The field of human-computer interaction tries to find ways to accommodate a number of functional and non-functional user requirements. Hence, this technical report focuses on reconciling the factors *fun*, *security*, and *embeddedness*. It reaches to give an overview on the interplay of gamification, usable security and embedded systems. The individual topics comprise a number of areas, such as smart watches, quantified self, or crowd-sourcing.

During the summer term in 2014, the Embedded Interactive Systems Laboratory at the University of Passau encouraged students to conduct research on the general topic of “Fun, Secure, Embedded”. Each student analyzed a number of scientific publications and summarized the findings in a paper.

Thus, each chapter within this technical report depicts a survey of specific aspects of a topic in the area of fun, secure, embedded interfaces. The students’ backgrounds lie in Computer Science, Interactive Technologies, Mobile and Embedded Systems, and Internet Computing. This mixture of disciplines results in a highly post-disciplinary set of viewpoints. Therefore, this technical report is aimed at providing insights into various aspects of current topics in Human-Computer Interaction.

Passau, October 2014

The Editors

Tobias Stockinger, Patrick Lindemann, Marion Koelle, and Matthias Kranz

Gamification of the Quantified Self

Stefan Bildl
Universität Passau
Innstr. 43
94032 Passau, Germany

bildl04@stud.uni-passau.de

ABSTRACT

Self-tracking using technology is a relatively new concept[3]. Since technology has enabled people to track themselves efficiently, the movement of the Quantified self gained much popularity.

This paper introduces the ideas behind the Quantified Self. In this movement of sensor based self-tracking, people use sophisticated tools in order to collect information about themselves.

The act of tracking can often get frustrating for the user[10], because of the manual effort that it requires. Quantified Self approaches need features that motivate the user and counteract this frustration that arises through the self-tracking task. This paper shows, how methods of Gamification can be applied to achieve this motivation and to make tedious activities more enjoyable. This work presents some of these concepts and later describes various applications in the different scenarios of the Quantified Self.

Keywords

Quantified Self, Gamification, Acceptance, User Experience, Big Data

1. INTRODUCTION

The Internet of Things emerges with increasing speed, as the number of sensor based systems that enter the consumer market rises accordingly. In 2008, the number of devices connected to the Internet even surpassed the number of humans living on the planet[14].

People now have the ability to automatically “track” themselves with the assistance of intelligent and sensor driven systems. A person’s body and also emotions can now be monitored easily, without the person doing much work for the data-gathering process. Logging health statistics, reviewing one’s progress in a certain sport or scheduling and tracking of one’s daily activities often become as easy as starting an application on a smartphone. Not only people with a strong interest in technology take part in the activity

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Advances in Embedded Interactive Systems ’14 Passau, Germany
Volume 2, Issue 3 (October 2014). ISSN: 2198-9494

of self-monitoring. A whole movement is arising around this concept. The Quantified Self Movement[10].

2. THE QUANTIFIED SELF

From running pace to emotions and moods, “Quantified Selfers”[3] track many day to day tasks with the aim to improve the parts of their lives, they are unhappy with. The point of Quantified Self systems is to help the users reach their own goals. People use sophisticated technology to gather information about themselves. The data helps them better understand activities and habits and assists at removing bad ones[8], as shown later in this paper. The Quantified Self applications also give tips on how to achieve goals.

The Quantified Self idea covers a whole lot of possible tracking-scenarios. Beyond capturing sport statistics or daily mood changes, there are other more serious applications of “quantifying” oneself. Quantified Self approaches can help addicts with getting off of drugs and help them live a healthy drug-free life. So called “eHealth” applications assist sick or vulnerable people with chronic diseases. Patients gather data about their symptoms with their smart devices and share their symptoms with other patients on health social networks[13]. Through Quantified Self, they are able to better communicate with the treating physician[10]. It is often the case that people only give information to the doctor, that they themselves see as relevant. Sometimes the patient leaves out symptoms that are essential for creating the right diagnosis. If the patient shows the doctor the objective data, which was tracked through a Quantified Self application, the doctor possibly sees patterns, that he else might not see. This can optimize the patients treatment and speed up the curing process. So with such applications, the patient-to-doctor communication can be improved[10].

Self-surveillance has different positive effects on the person using it. Quantified Self gadgets support users in understanding their habits, thoughts and behaviors. Users gain self-insight and increase self-control. Quantified Self applications also promote positive behaviors of the user[9]. These applications remove negative aspects of a persons life, like addictions or bad habits.

The principles of monitoring oneself have negative side effects, too. There is a trade-off, that occurs between quality of data collected with Quantified Self systems and usability and user-experience[10]. If the quality of data is high, then it is harder to capture. That means that with increasing complexity of information, the effort that has to be put into collecting this data rises, too. Information, which is easily

collectible is also often not very representative and much more general than information about specific aspects. The more time and effort the user has to put into a Quantified Self system just to track something, the more frustrating and demotivating the Quantified Self approach may become[10].

The phenomena of “gamifying” applications has become a big trend recently[5]. Through simple game mechanics, the usability and user experience of Quantified Self applications can be enhanced. Tedious activities can be made enjoyable through the application of Gamification[15]. In the next section the concepts of Gamification are defined.

3. GAMIFICATION

It is sometimes required, that the user actively contributes to the data-gathering process. Because of the increased effort which this requirement implies, users may easily become frustrated. To counteract this frustration, system designers incorporate game elements into the data-collection task of the Quantified Self system. This makes the whole application more attractive and appealing for the user.

Gamification is defined as “the use of video game elements in non-gaming systems to improve user experience”[6]. In contrast to real games or “serious games” (which is a full-fledged game for the purpose of education), applications that utilize Gamification concepts, “merely incorporate”[4] elements of games. “Gamified” systems are not used for entertainment purposes only. When it comes to Quantified Self products, Gamification is used heavily to make the process of information-collection more enjoyable and fun for users. A popular successful example of a gamified Quantified Self application is Nike+. Such Quantified Self applications benefit from the positive effects of Gamification[11].

Through Gamification, Quantified Self systems are not only useful, but also become enjoyable to use. Gamification principles motivate the user to use the Quantified Self system long term. This is because game elements not only generate extrinsic motivation (usefulness), but also intrinsic motivation (fun). With those two motivating factors combined, the intention of using the system in the future is enforced[11] by the utilization of Gamification techniques. This means that enjoyable and “fun” interfaces are important for the user satisfaction. So Gamification can be used to fulfill the intrinsic needs of a user.

In the next section, game elements which can be used in the task of “gamifying” an application, are presented.

Methods of Gamification

As defined by Reeves and Read, there are special “ingredients” [12] of a good game. These ingredients include self-representation with avatars, marketplaces and economies, three-dimensional environments, narrative context, feedback, ranks and levels, reputations, competition under rules, parallel communication systems, and time pressure.[12] Some of these ingredients are also applicable for Quantified Self products. So what can be used in Quantified Self products?

Avatars.

Avatars are figures that are mostly used in roleplaying games[5]. These represent the player in the virtual world of the game. Quantified Self applications could feature avatars and a way to customize these little virtual selves. The gamified system could possibly reward the users achievements

with virtual loot[15] like outfits or accessories for the avatar. Because an avatar is a representation of people's real identities, many users put much effort into creating a figure, that represents their style. The user starts to build up an emotional attachment to the avatar[16]. Customization is therefore a way to better their relationship with their avatar. Also, with increasing effort the user puts into it, the more solid this attachment gets. Avatars can keep the person “in the game” and persuade him/her to stay in the self-tracking-process. Avatars are also a way to represent the user's progress in the Quantified Self application. Watching the Avatar leveling up and completing quests is additionally more appealing than watching the progress in a menial everyday task[15]. So avatars can be really useful in Quantified Self applications.

Feedback.

The system should inform its user about how well he/she is doing in the platform[7]. Feedback makes the progress visible for the user and helps him achieve his goals. Also motivation rises easily, if there exists positive feedback[15].

An example of successful feedback mechanisms would be the so called “Live Interest Meter”, that was developed to help lecturers improve their presentation skills and to make the lectures much more interesting. In this context, the listeners of the lecture use a smartphone app to evaluate the presentation. Through feedback the audience provides, the presentation-style can be adapted to their wishes[11].

Badges and Trophies.

Rewarding a user for his/her achievements with trophies or badges is another method of Gamification. Users could, after finishing a challenge, review the earned rewards.

This generates the feeling of pride for the person who accomplished something. Achievements and badges thus generate good feelings in the user. Only the perception of the peak and end of an event in the past significantly affect the reinterpretation of it later, when it is remembered[2]. So if positive feelings occur after/at the end of for example the sportive activity that is tracked, then the person is happier with the made progress and is more likely to proceed with the self-improvement process and self-tracking. As said earlier, motivation can rise easily if there exists positive feedback. It helps the person reach more of the goals, that the “gamified” application sets up. Also other people, who are viewing the profile of a successful Quantified Self user become motivated because they want to compete with said user.

In the example of the Live Interest Meter that was introduced previously in this paper, badges and trophies are used to decorate the “Knowledge Tree”, which represents the lecture. The lecturer can then, after the lecture, see in this animated tree, how well he is doing and how the audience reacted to him. He can change his style of presentation accordingly and through the feedback of the audience, it becomes determinable, if the change made the presentation's quality better or worse[11].

Communication.

A system-wide communication channel[12] also improves the user experience. Through creating a platform, where people can chat with each other or help each other out, a community can be established. This community fulfills the need of relating to other like-minded people. By satisfy-

ing this intrinsic need[1] of human beings, the user does not feel alone anymore and can share their progress with others. Also the intention of users to visit the community of a (Quantified Self-) system is higher, if Gamification methods are used[11].

Ranks and Levels.

Ranks and levels can represent the overall progress of the user of a Quantified Self system. Through ranking lists and scores, the user can see the effects of the self-improvement process. He/she can compare current scores with their previous ones and thus view their progress after a certain amount of time.

Time pressure.

Time constraints can motivate further. Time pressure brings the maximum out of the user's performance in sports. Why not use this as a Gamification method for Quantified Self applications?

The aspect of time pressure is for example used in the application of the Quitbit Lighter¹. This electronic lighter measures the time, that has passed since the user has lit his/her last cigarette. The user can decide how much time he wants to wait until he smokes the next one. Through gradually increasing the time between cigarettes, the user can reduce his/her urge to smoke.

4. EXISTING APPLICATIONS AND SCENARIOS OF THE QUANTIFIED SELF

4.1 Fitness trackers

The main sector of Quantified Self is the one of health and fitness applications. There already exist a number of such systems on the consumer market.

Wristband sensors are pedometers that passively count the user's steps taken throughout the day. The most popular Quantified Self wristbands are the Nike+ Fuelband SE and the Jawbone UP[14]. These rubber wristbands have built in accelerometers which collect data in the background, while the user is moving with the device worn around his/her wrist.

These sensor systems pair with smartphones, which allow the user to interact with an touch-screen interface. Through fitness apps on smartphones, the statistical data that was gathered with the wristband can be presented in an enjoyable way to the user. These apps use Gamification principles like feedback, badges, achievements, scores or leaderboards. Feedback can keep a user in the continuous process of self-tracking. As A. Calvo suggests, this is the case, because the reinterpretation of an event in the past is significantly affected by the feelings and emotions of the actor during the peak and the end of said event[2]. Through badges, achievements and motivational messages, the user interfaces of the fitness trackers achieve these positive emotions in the user because they provide intrinsic value[4] and thus they motivate the user to "keep playing".

As shown in figure 1, smartphone-applications for self-tracking provide feedback and visualize the progress through diagrams. Also they give tips on how to achieve ones goals(See

¹<http://quitbitlighter.com/>

"try this"-tip shown on the left screen in figure 1). Also community is established through such applications. On figure 1, the "UP Feed" is shown, where one can see activities or meals that friends have tracked with their Jawbone UP and the smartphone application.



Figure 1: The interface of the Jawbone UP.
Source: <http://www.gizmodo.com.au/> visited 06.06.2014.

Communities fulfill the intrinsic need of relatedness of humans[1], and enable the user of a Quantified Self system to exchange thoughts with friends. Also users can help each other out, when problems in self-tracking or the sport arise. Also community can start competition between members.

This competition can be strengthened through leaderboards and ranking systems[7], which for example Nike+ provides². Ranking systems in the fitness applications also help making the progress tangible for users. Runners that use applications with such ranking mechanisms can compare the current run to previous ones and thus determine, how much their fitness changed over time.

The Gamification principles that are used in these fitness applications enhance the user experience and satisfaction and motivate the user to use the application further[11].

4.2 Health tracking/medicine

The Quantified Self concepts are not only used in fitness applications. They are also applied in the treatment of long-term illnesses and health conditions[10].

Since illnesses like asthma or diabetes require strong self-management, patients need an efficient way to keep track of their symptoms.

Such systems should inform the user about possible hazards. A application that assists asthma patients can warn about pollen or pollution in the air. This can prevent asthma attacks and thus these systems can be really helpful for preserving the patient's life quality[10].

Tools for tracking blood sugar can help people with diabetes. Some of the health related Quantified Self applications also make use of Gamification. The "Diabetes Companion" app by mySugr is an example. This smartphone app lets the user measure blood sugar (with external hardware), while using game elements like scores and challenges. Additionally an avatar called "The Monster" playfully and constantly reminds the user to track health statistics³.

A study by K. Huckvale and C. Morrison shows that

²<https://secure-nikeplus.nike.com/plus/> visited 04.06.2014

³<http://mysugr.com/companion/> visited 05.06.2014

people successfully use smartphone apps for the purpose of tracking health conditions over time[10]. But the study also shows that many users do not use all of the features provided by the applications(“Feature use was minimal”[10]). In the study, it also “seemed that the process was as important as the resulting numbers”[10].

With this said, one might be able to improve the process of tracking by using the previously explained Gamification techniques.

Quantified Self in health related social networks

Some health related social networks like PatientsLikeMe, CureTogether, MedHelp, or SugarStats feature Quantified Self-tracking. In these networks, patients can note their symptoms, their treatments and other biological information into easy-to-use tracking systems[13]. Patients can make their symptoms and the progression of the illness visible on their profile. Through systems like these, valuable information about treatment efficiency can be gained. For example CureTogether lets its users see the top treatment of their disease[13]. Through the communities behind such applications, patients can talk to each other and exchange tips on how to deal with the illness. Also such systems enable users to print out their symptoms and health statistics. They can then show the information to the doctor which improves patient to doctor communication[10].

Wearable sensors

There exist a number of wearable health-tracking sensor systems. A promising approach are electronic tattoos, that can monitor vital signs of the user continuously[14]. As shown in figure 2, these tattoos are stretchable and thus do not restrict the movement of the wearer.

These flexible patches are able track information like heart-rate, brain activity, body temperature and hydration levels and can wirelessly transmit the gathered information[14]. Other applications of the new patches include the continuous monitoring of blood-pressure or glucose levels. Last can be very useful for diabetics, who constantly have to check their blood sugar.

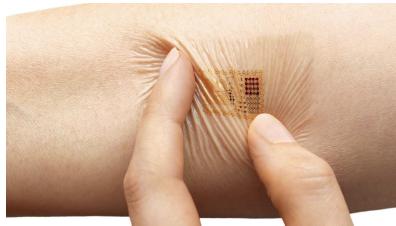


Figure 2: Electronic tattoo monitors vital signs

Source: <http://www.electronicproducts.com/> visited 08.06.2014

In the future, people might have a greater understanding of the human brain. Mental performance optimization, emotion- reading, -mapping and -management programs could become useful applications[14]. Consumer EEGs are a early form of brain-data obtaining sensor systems, that are presently used. Devices like the NeuroSky wearable EEG biosensor-headset (Figure 3) have been used with the aim to improve attention, meditation or video game performance[14]. Since

devices that measure EEG are now affordable, they might soon be used in various other applications.



Figure 3: The NeuroSky Headset

Source: <http://www.thinkgeek.com/product/e9e5/> visited 08.06.2014

Other health related applications

The cessation of an addiction often fails because of lacking motivation to change. With applications like the Quitbit lighter⁴, smokers who want to give up smoking can use this lighter to track their progress. The lighter is a simple application, that shows the user on its LED display, how much time has passed since the last cigarette. When the lighter is used, this time is reset to zero. To view the progress made, the user is able to use a smartphone app that is connected to the lighter. This application presents statistics about how often the user has smoked in the past week, month or during three months. As said earlier, feedback motivates the user of a Quantified Self system to keep going. Through seeing the made progress, it becomes easier for the smoker to motivate him-/herself to not give up.

Mood tracking is also a possible tracking-scenario of Quantified Self systems[3]. The application Mood Panda is an example for such a system. This web-application is also available as a smartphone app. The program allows users to track their mood in a scale from one to ten and leave a tweet-like message about the factors that currently influence their mood. Also the community behind the system helps out people with bad mood. These programs can be used by people with depression and other psychological disorders to track their mood changes over time.

5. CONCLUSIONS

Quantified Self systems can be useful in many different contexts. As the sensors and data-gathering devices that are used for these applications evolve through the technological progress, these applications get more and more popular. Quantified Self applications let users reflect on their lives. These systems help users with improving fitness and health and show, how they can stop bad habits and addictions. To make these systems more enjoyable to use, the powerful tool of Gamification can be utilized. Game elements enhance the user experience and fulfill the intrinsic needs of users. Because of Gamification and the intrinsic motivation that it generates, users are motivated to use self-tracking systems long term.

⁴<http://quitbitlighter.com/> visited 08.06.2014

6. REFERENCES

- [1] A. F. Aparicio, F. L. G. Vela, J. L. G. Sánchez, and J. L. I. Montes. Analysis and application of gamification. In *Proceedings of the 13th International Conference on Interacción Persona-Ordenador*, INTERACCION '12, pages 17:1–17:2, New York, NY, USA, 2012. ACM.
- [2] R. A. Calvo and D. Peters. The irony and re-interpretation of our quantified self. In *Proceedings of the 25th Australian Computer-Human Interaction Conference: Augmentation, Application, Innovation, Collaboration*, OzCHI '13, pages 367–370, New York, NY, USA, 2013. ACM.
- [3] E. K. Choe, N. B. Lee, B. Lee, W. Pratt, and J. A. Kientz. Understanding quantified-selfers' practices in collecting and exploring personal data. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, pages 1143–1152, New York, NY, USA, 2014. ACM.
- [4] S. Deterding. Gamification: Designing for motivation. *interactions*, 19(4):14–17, July 2012.
- [5] S. Deterding, D. Dixon, R. Khaled, and L. Nacke. From game design elements to gamefulness: Defining "gamification". In *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, MindTrek '11, pages 9–15, New York, NY, USA, 2011. ACM.
- [6] S. Deterding, M. Sicart, L. Nacke, K. O'Hara, and D. Dixon. Gamification. using game-design elements in non-gaming contexts. In *CHI '11 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '11, pages 2425–2428, New York, NY, USA, 2011. ACM.
- [7] L. Galli, P. Fraternali, and A. Bozzon. On the application of game mechanics in information retrieval. In *Proceedings of the First International Workshop on Gamification for Information Retrieval*, GamifIR '14, pages 7–11, New York, NY, USA, 2014. ACM.
- [8] I. Li, J. Forlizzi, and A. Dey. Know thyself: Monitoring and reflecting on facets of one's life. In *CHI '10 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '10, pages 4489–4492, New York, NY, USA, 2010. ACM.
- [9] I. Li, Y. Medynskiy, J. Froehlich, and J. Larsen. Personal informatics in practice: Improving quality of life through data. In *CHI '12 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '12, pages 2799–2802, New York, NY, USA, 2012. ACM.
- [10] J. Meyer, S. Simske, K. A. Siek, C. G. Gurrin, and H. Hermens. Beyond quantified self: Data for wellbeing. In *CHI '14 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '14, pages 95–98, New York, NY, USA, 2014. ACM.
- [11] B. S. Morschheuser, V. Rivera-Pelayo, A. Mazarakis, and V. Zacharias. Interaction and reflection with quantified self and gamification: an experimental study. In *Special Edition: Papers from the 2013 PLE Conference Personal Learning Environments: Learning and Diversity in Cities of the Future*, page 117.
- [12] B. Reeves and J. L. Read. *Total engagement: How games and virtual worlds are changing the way people work and businesses compete*. Harvard Business Press, 2013.
- [13] M. Swan. Emerging patient-driven health care models: an examination of health social networks, consumer personalized medicine and quantified self-tracking. *International journal of environmental research and public health*, 6(2):492–525, 2009.
- [14] M. Swan. Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0. *Journal of Sensor and Actuator Networks*, 1(3):217–253, 2012.
- [15] J. R. Whitson. Gaming the quantified self. *Surveillance & Society*, 11, 2013.
- [16] J. Wolfendale. My avatar, my self: Virtual harm and attachment. *Ethics and Information Technology*, 9(2):111–119, 2007.

Präventionstechniken gegen Phishing

Anna Eiberger
Universität Passau
94032 Passau, Deutschland
eiberg01@stud.uni-passau.de

ABSTRACT

Phishing ist eine Angriff auf die persönlichen Daten von Internetnutzern. Betrüger täuschen ihre Opfer um ihnen Zugangsdaten, wie Benutzernamen, Passwörter und Online Banking Informationen, zu entlocken. Die Täter benutzen zum Sammeln der Daten gefälschte E-Mails und Webseiten, welche die Informationen an einen ausgewählten Server weiterleiten. Mittlerweile gilt Phishing als organisierte kriminelle Aktivität. In diesem Paper präsentiere ich verschiedene Methoden zur Erkennung und Vorbeugung solcher Angriffe, nämlich Verschlüsselung durch SSL Zertifikate, Machine Learning Classifier und Einmal Passwörter. Im Anschluss gehe ich noch auf Präventionstechniken für mobile Geräte, wie Smartphones und Tablets ein.

Keywords

Phishing, Identitätsklau, Vorbeugung, Effektivität

1. EINLEITUNG

Ein Phishing Angriff ist eine Kombination aus „social engineering“ und technischer Manipulationsmethoden, um Internetnutzer zu überzeugen, sensible Informationen von sich preis zu geben [5]. Dazu werden gefälschte Webseiten oder E-Mails verwendet. Das Ziel des Angreifers ist es mit den gestohlenen Daten, wie beispielsweise Benutzernamen, Passwörtern oder Online Banking Informationen, Geld zu verdienen [5]. Ein typisches Beispiel dafür ist ein Angriff gegen eBay Kunden [15]. Der Vorgang beginnt mir einer E-Mail an den Nutzer. Darin wird er aufgefordert seine Account Daten unter dem bereitgestellten Link zu ändern, da diese angeblich abgelaufen sind. Es sieht aus, als käme die Nachricht von S-Harbor@eBay.com und der Link verweist offensichtlich auf cgi1.ebay.com, tatsächlich aber wird das Opfer auf einen Server nach Südkorea geleitet, welcher in keinerlei Beziehung mit eBay steht. Der Klick auf den Link erzeugt eine scheinbar seriöse Internetseite, mit dem eBay Logo und dem üblichen Design der Seite. Nun sollen persönlichen Informationen, wie Kreditkartendaten, Sozialversicherungsnum-

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Advances in Embedded Interactive Systems '14 Passau, Germany
Volume 2, Issue 3 (October 2014). ISSN: 2198-9494

mer, eBay Benutzername und Passwort eingegeben werden. Die Bestätigung erfolgt, wenn der Nutzer auf den Submit-Button klickt. Seine Daten werden an den feindlichen Server gesendet, wo die Phisher die Informationen sammeln und benutzen.



Figure 1: Statistik über aktuelle Phishingangriffe

Wie die Abbildung 1¹ zeigt, ist Phishing per E-Mail die meist verwendete Methode, sensible Daten von Nutzern zu stehlen. Die Frage ist, wieso immer noch so viele Menschen dieser Strategie zum Opfer fallen? Gemäß der APWG² (Anti Phishing Working Group) taucht der Begriff „phishing“ erstmals 1995 auf. Damals schon benutzten Betrüger E-Mails als Lockmittel, um Passwörter und Bankinformationen aus dem Meer von Internetnutzern zu „fischen“ [3]. Das Paper „Why Phishing Works“ [2] beschreibt dazu drei Faktoren, die von Angreifern ausgenutzt werden:

1. Fehlendes Wissen über Computer- und Sicherheitssysteme. Wenig Nutzer kennen Indikatoren an denen man sichere Webseiten erkennt. Viele haben Probleme diese

¹<http://de.statista.com/statistik/daten/studie/150871/umfrage/am-haeufigsten-von-phishing-betroffene-organisationen/>, abgerufen am 10.06.2014

²<http://www.antiphishing.org/about-APWG/>, abgerufen am 10.06.2014

- richtig zu interpretieren. Zum Beispiel wissen anfängliche Internetbenutzer selten, dass eine Seite mit SSL Verschlüsselung gesichert ist, wenn in der Browser leiste das Symbol eines geschlossenen Vorhängeschlosses erscheint. Ein weiteres Problem stellen die SSL Zertifikate dar. Nur wenige wissen wie man Diese überprüft oder verstehen den Inhalt nicht richtig.
2. Visuelle Täuschung mit gefälschten Bildern, Texten und Eingabefenstern. Eine beliebte Methode unter Phishern ist das Austauschen von einzelnen, sich ähnelnden Buchstaben in Domain Namen. Beispielsweise wird bei „www.paypal.de“ der Buchstaben „l“ mit die Zahl „1“ ausgetauscht. Nur Nutzer die achtsam sind, haben eine Chance, solch einen gefälschten Link zu erkennen. Manche Täter verwenden Bilder von Hyperlinks, welche einen aber nicht zu der echte, von ihren Opfer erwarteten Internetseite, sondern zu einer anderen, eben einer betrügerischen Webseite leiten.

3. Fehlende Aufmerksamkeit und geringes Bewusstsein für Sicherheitsindikatoren. Der Schutz vor Angriffen ist für Internetnutzer oft ein zweitrangiges Ziel. Auf ihre Arbeit konzentriert, können Warnmeldungen oder deren Abwesenheit schnell unbemerkt bleiben. Selbst Nutzer die wissen, dass sie auf Verschlüsselungssymbole achten müssen, werden oft getäuscht, da sie deren Position zu wenig beachten. Manche Angreifer positionieren optische Sicherheitshinweise auf ihren Internets Seiten, welche Nutzer als echt interpretieren.

Es ist sozusagen ein Kampf zwischen Phishern und Anti-Phishern, um die Benutzeroberfläche. Ein erfolgreicher Angreifer muss seinen Opfern nicht nur glaubwürdige Webseiten präsentieren, der Auftritt muss außerdem so bestechend sein, dass der Nutzer die im Browser installieren Sicherheitsindikatoren nicht bemerkt [2].

Der Rest des Papers ist wie folgt strukturiert. Ich stelle ausgewählte Präventionstechniken gegen Phishing vor, wie beispielsweise eine Verschlüsselung von sensiblen Daten per SSL Zertifikate. Danach präsentiere ich die Effektivität dieser Strategien, die man anhand von Benutzerstudien evaluiert und schließlich berichte ich noch über die Übertragung solcher Sicherheitsindikatoren auf mobile Geräte.

2. PRÄVENTIONSTECHNIKEN

Es gibt zahlreiche Sicherheitssysteme die durch unterschiedlichste Prinzipien versuchen gefälschte Webseiten zu erkennen und den Nutzer durch Techniken, wie beispielsweise eine farbige Browser leiste, zu warnen dort persönliche Daten von sich einzugeben [7]. Im Folgenden stelle ich einige Techniken vor.

2.1 Warnsysteme auf SSL-Basis

Eine EV SSL (Extended Validation Secure Socket Layer) Verbindung stellt eine interaktive Bestätigung und Entschlüsselung der Server-Client-Beziehung bereit. Dem Nutzer wird damit die Erkennung von sicheren Servern erleichtert, da zusätzliche Informationen des EV Zertifikats bei der Verbindung übertragen werden. Mit eingeschlossen, Standort der Gesellschaft, Firmenname und eine Registrierungsnummer des Servers der Webseite [13]. In dem Paper „Shining Chrome: Using Web Browser Personas to Enhance SSL Certificate Visualization“ [9] wird ein Plugin namens Personas

vorgestellt, das von EV SSL Gebrauch macht. Es soll Internetnutzern helfen gefälschte Webseiten zu erkennen. Hierfür wechselt der Hintergrund der Browser leiste je nach Sicherheitsstufe seine Farbe. Das Gesamtlayout bleibt dabei unverändert um mögliche Verwirrungen oder Ablenkungen der Benutzer durch das Plugin zu minimieren.

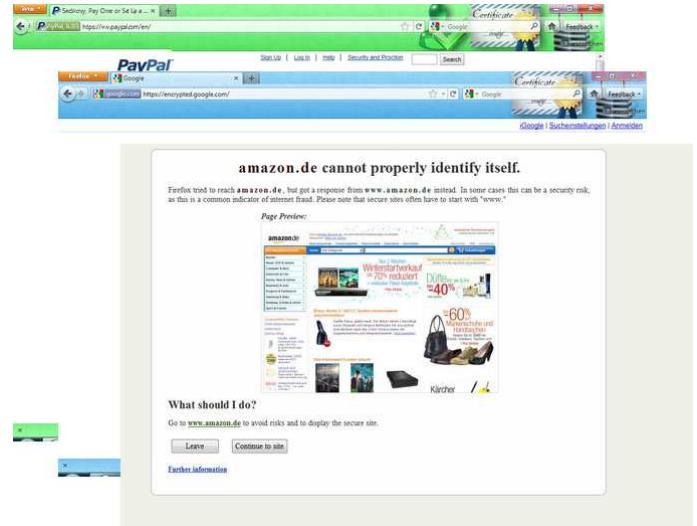


Figure 2: Sicherheitsstufen von SSL Personas

Die Abbildung 2³ zeigt die Sicherheitsindikatoren von Persona. Die erste Stufe zeigt ein in grün hinterlegtes Fenster mit drei Sicherheitssymbolen (grüner Hacken, Zertifikat, geschlossenes Vorhängeschloss) im Hintergrund. Das bedeutet, dass die Webseite auf die gerade zugegriffen wird, EV SSL Zertifikate benutzt und somit sicher verschlüsselt ist. Im zweiten Fenster ist ein blauer Hintergrund mit nur noch zwei Sicherheitssymbolen zu sehen, was eine Verschlüsselung mit Standard SSL Zertifikaten impliziert. Das dritte Bild ist eine Warnmeldung die erscheint, wenn bei der Überprüfung einer Internetseite aufgefallen ist, dass deren Zertifikat für eine Domain verwendet wird, für die es nicht ausgestellt wurde. Zusätzlich zeigt die Meldung ein Bild von der blockierten Seite, ohne diese wirklich zu laden. Der Nutzer kann nun entscheiden, ob er die Seite verlassen oder damit fortfahren will. Möglicherweise handelt es sich bei so einem Fall um eine gefälschte Webseite.

2.1.1 Benutzbarkeit von SSL Zertifikaten

Im Rahmen der Entwicklung von Persona wurden zwei Benutzerstudien durchgeführt, deren Ergebnisse ich kurz zusammengefasst habe [9].

Die Teilnehmer, überwiegend Studenten, bekamen eine Liste mit verschiedenen Webseiten, die unterschiedliche Sicherheitseigenschaften hatten (von EV SSL Verschlüsselung bis Phishing). Das Ziel ist es, dass Nutzer mit dem Plugin alle Webseiten klassifizieren und sich somit vor gefälschten Seiten schützen können. Teilnehmer die unbekannte Seiten besuchten achteten mehr auf das Plugin, als bei ihnen bekannten Seiten, somit wurden fremde Seiten erfolgreich klas-

³<http://www.softbuz.com/windows/network-internet/mozilla-extensions/screenshots/sslpersonas/>, abgerufen am 07.06.2014

sifiziert. Allerdings war die Bearbeitungsdauer viel zu kurz um sich an das Plugin zu gewöhnen. Nach sieben Monaten in denen Persona zum Download bereit stand, wurde es mehr als 15000 mal heruntergeladen. Eine Online Befragung der Nutzer ergab, dass weniger als 10% der Teilnehmer weiblich sind. Fast die Hälfte der befragten Personen beschrieben sich als fortgeschritten Benutzer, nur 2% stuften sich als Anfänger ein.

2.1.2 Problematik mit SSL Zertifikaten

Warum die Zahl der unerfahrenen Benutzer so gering ist, lässt sich wohl damit erklären, dass Websicherheit nicht das primäre Ziel von vielen Internetnutzern ist. Es fehlt das Interesse an Sicherheitsapplikationen, nur wenige informieren sich über diese Thematik. Dazu kommt noch die steigende Komplexität der Zertifikate [9], denn nur dadurch kann eine sichere Verschlüsselung gewährleistet werden. Nutzer haben oft nicht die Motivation sich entsprechende Kenntnisse anzueignen um Zertifikate zu verstehen.

2.2 Machine Learning Classifier

Eine weitere Technik um Phishing entgegen zu wirken, ist die Benutzung von Machine Learning Classifier (MLC). Allgemein basieren MLC auf einem Algorithmus (Classifier), der versucht mit einer speziellen Funktion Inputs zu gewünschten Outputs zu verarbeiten [1]. Bei der Klassifikation von Webseiten, wird ein Algorithmus verwendet, der gefälschte Seiten, anhand von bestimmten Merkmalen, wie dem URL, Inhalt und Herausgeber der Seite erkennt [14]. Eine Art von MLC ist URL filtering, dabei erfolgt die Identifikation gefälschter Webseiten per Abgleich des URLs einer Seite mit einer Blacklist [10]. Eine solche Liste ist die vollständigste Auflistung von bekannten Adressen von Phishingseiten, die verfügbar ist [14]. Die Effektivität einer Blacklist wird mittels folgender drei Indikatoren gemessen, Vollständigkeit, Fehlerquote und Aktualität [14]. Ein Zeiterlust von nur wenigen Stunden kann die Qualität erheblich senken, sodass sich der Nutzer nicht mehr sicher auf die Liste verlassen kann [14]. Eine andere Herangehensweise ist eine Lösung mit Heuristiken. Ein Algorithmus entscheidet, basierend auf Nutzererfahrung, ob eine Seite vertrauenswürdig ist oder nicht [10]. Eine solche Lösung verwendet mehrere Heuristiken und konvertiert die Ergebnisse von jeder Heuristik in einen Vektor. Basierend auf diesem Vektor wird die Wahrscheinlichkeit, dass eine Seite eine gefälschte ist, berechnet und dann mit dem festgelegten Grenzwert des Urteilsvermögens verglichen. Nach Angaben des Papers „An Evaluation of Machine Learning-Based Methods for Detection of Phishing Sites“ [10] ist das Tool namens CANTINA das erfolgreichste im Kombinieren von Heuristiken. Die Wahrscheinlichkeit, dass eine Webseite gefälscht wurde, wird dabei mit einer gewichteten Mehrheit aus acht Heuristiken kalkuliert. Es werden dazu das Alter der Domain, bekannte Bilder, verdächtige URLs und Links, die IP-Adresse, Punkte im URL und TF-IDF-Finale Heuristiken, verwendet. Anders wie beim URL filtering, ist es mit dieser Methode möglich, unbekannte Phishingseiten zu identifizieren [10].

2.2.1 Benutzbarkeit

Anti-Phishing Toolbars sind universell verfügbar und werden üblicherweise von anfänglichen Computernutzern verwendet [1]. Es gibt viele verschiedene Ausführungen und damit auch einige unterschiedliche Erkennungsstrategien, die

kaum aufeinander abgestimmt sind, was wenig benutzerfreundlich ist [10]. Obwohl diese Toolbars helfen, dass Phishingproblem abzuschwächen, haben viele Studien die Ineffektivität solcher Techniken gezeigt [1]. Im nächsten Abschnitt „2.2 Problematik mit machine learning classifier“ gehen ich darauf genauer ein.

2.2.2 Problematik mit machine learning classifier

Das Hauptproblem ist, dass der gefälschte Link oft ohne Betrachtung des Zusammenhangs, in dem er dem Nutzer präsentiert wurde, getestet wird. Dadurch geht Genauigkeit bei der Klassifikation verloren, weil der Bezug zur Herkunft der Adresse fehlt [1]. Ein anderes Problem ergibt sich, wenn der Nutzer tatsächlich auf eine Phishingseite stößt. MLC verbinden den Nutzer sofort mit der ausgewählten Webseite, sobald der Link angeklickt oder in die Adressleiste eingegeben wurde. Der Benutzer ist dann jeglichem Angriff dieser Seite, ausgesetzt [1]. Ein weiteres grundlegendes Problem, dass in früheren Forschungsarbeiten auftritt, ist das Verhältnis der Erkennungsmerkmale von Phishing Webseiten und E-Mails. Die Anzahl der Charakteristika für gefälschte Webseiten ist geringer als die für gefälschte e-Mails, somit ist die Ermittlung von Phishing Webseiten mit Hilfe von MLC im Gegensatz wesentlich schwieriger [10]. Das kann auch daran liegen, weil gefälschte Internetseiten eine extrem kurze Lebensdauer von nur wenigen Tagen haben, was eine Führung einer möglichst aktuellen Blacklist schwierig gestaltet [14].

2.3 Einmal-Passwörter

Es gibt spezielle Seiten im Internet die zufällige Einmal-Passwörter generieren. Das Paper „Preventing Phishing Attacks using One Time Password and User Machine Identification“ [3] beschreibt diesen Vorgang. Um ein sicheres Passwort zu bekommen, benötigt man einen Account bei einer entsprechenden Webseite und muss zusätzlich eine Handynummer oder alternative E-Mail Adresse angeben, um das Passwort abrufen zu können. Zusätzlich wird ein verschlüsseltes Zeichen (token) am Rechner des Nutzers und in der Datenbank des Servers abgespeichert. Eine sichere Dekodierung der verschlüsselten Zeichen gewährleistet die PKIEncrypt (Public Key Infrastructure) Funktion, dessen Cookie nur für jeweils 15 Minuten gültig ist und unter anderem die IP Adresse des benutzen Rechners speichert. Das Cookie wird über verschlüsselte Kanäle übertragen und ist außerdem mit dem X509Certificate2 Zertifikat gesichert. Der Zugang zur gewünschten Webseite erfolgt mit dem Einmal-Passwort und dem gültigen token [3].

2.3.1 Benutzbarkeit von Einmal-Passwörtern

Für manche Nutzer ist dieses Szenario eher wenig attraktiv, da es zeitaufwändig ist, weil für jeden Login erst ein Einmal Passwort erstellen werden muss. Der Vorteil ist, dass Angreifer, welche die Webseite für das Generieren der Einmal-Passwörter fälschen, damit keinen Schaden verursachen. Die Passwörter können nämlich nur auf dem Handy oder unter der zweiten E-Mail Adresse des berechtigten Nutzers abgerufen werden [3].

2.3.2 Problematik mit Einmal-Passwörtern

Falls der Angreifer allerdings durch so eine Phishingattacke die Anmeldeinformationen bekommt, kann er sein Opfer mit SMS und E-Mails überfluten, was viel Ärger anrichtet. Um so eine Nachrichtenflut zu verhindern, sollte der Nut-

zer das Programm CAPTCHA verwenden. Es schützt vor Computersoftware, die ohne menschliche Interaktion arbeiten kann und automatisch wiederholende Aufgaben erledigt, wie zum Beispiel E-Mail Adressen sammeln und Nachrichten verschicken. CAPTCHA erstellt Tests, welche nur von Menschen absolviert werden können und bewertet diese im Anschluss. Aktuelle Computerprogramme würden so einen Test nicht bestehen, aufgrund von fehlender Intelligenz. Ein Beispiel wäre ein verdrehter Text [3].

3. PHISHING AUF MOBILEN GERÄTEN

Alle genannten Präventionsmethoden beziehen sich bislang nur auf den Schutz von Computern, aber das Phishingproblem lässt sich nicht mehr darauf beschränken. In den letzten Jahren wurden Handys immer mehr als Kommunikationsmethode benutzt, nicht nur zum privaten Zweck, sondern auch im Beruf. Deshalb werden Angriffe auf Smartphones für Hacker immer interessanter. Phisher nutzen verschiedene Schwachstellen von SMS, Wi-Fi Netzwerken und MMS aus [11].

3.1 Gefahren für Nutzer

Der Austausch von Informationen übers mobile Internet, ist nichts außergewöhnliches mehr. Man nimmt sein Smartphone oder Tablet und benutzt teilweise bedenkenlos öffentliche Netzwerke um eine Verbindung zum Internet herzustellen. Eine solche Verbindung ist aber ein Sicherheitsrisiko, weil Informationen die auf dem mobilen Gerät gespeichert sind, durch die Quelle gehackt werden können [11]. Eine Bedrohung der Privatsphäre kann auch durch installierte Applikationen (Apps) ausgelöst werden. Dafür muss eine App nicht zwangsläufig bösartig sein, aber sie kann es, durch das Sammeln einer großen Menge von persönlichen Daten, werden [11]. Es gibt Schadprogrammen in Form von Applikationen, so genannte Mobile Malware. Diese werden speziell für mobile Geräte und Plattformen entwickelt. Der Angriff erfolgt meistens in drei Phasen, zuerst wird der Host infiziert, dann führt der Angreifer seine Ziele aus und letztlich verbreitet er seinen Angriff. Eine solche Infektion kann bei folgende Aktionen passieren: Herunterladen einer schädlichen Datei, Besuchen einer Phishingwebseite, Teilen von Applikationen per Peer-to-Peer, Teilen von Links innerhalb einem mobilen Netzwerk und Synchronisieren mit dem Cloud Service [11].

3.2 Präventionstechniken für mobile Geräte

Es ist viel komplexer ein Smartphone zu sichern, das mit verschiedenen Netzwerken arbeitet, als einen PC. Die Auswahl an Sicherheitstools für mobile Geräte ist dementsprechend deutlich geringer, als für Computer [6]. Eine verbreitete Methode zum Schutz vor Phishing auf Smartphones, basiert auf dem Prinzip von Einmal Passwörtern. Ein Paradebeispiel hierfür ist mTan (mobile Transaction Authorization Number). Es wird für die Authentifizierung, beispielsweise bei Online Banking Diensten, verwendet. Der Vorgang ist ähnlich, wie der auf dem Computer. Der Nutzer muss sich bei einer entsprechenden Seite registrieren und seine Handynummer angeben. Er bekommt das Passwort dann per SMS zugeschickt und kann es nur für einen Login-Vorgang benutzen [12]. Leider ist dieses System nicht besonders sicher, was an zwei Faktoren liegt [12]. Erstens, stützt sich die Sicherheit der SMS Einmal Passwörter auf die Vertraulichkeit von SMS Nachrichten, die wiederum verlässt sich auf die Sicherheit von Mobilnetzwerken. Da es aber schon mehrere Angriffe auf

GSM- und 3G-Netze gab, kann diese Vertraulichkeit nicht gewährleistet werden. Zweitens, haben Kriminelle spezialisierte Handy-Trojaner entwickelt und verbreitet, weil viele Dienste auf SMS Einmal Passwörter umgestellt haben um ihre Transaktionen zu sichern. Solche Trojaner fangen SMS Nachrichten ab, die Einmal Passwörter enthalten. Außerdem gibt es Schadsoftware, die ihre Informationen über Touchscreens von Geräten sammeln. Als Lösung dafür, stellt das Paper „ScreenPass: Secure Password Entry on Touchscreen Devices“ [8] das System ScreenPass vor. Das ist eine Spezialsoftware, welche für die Eingabe von sensiblen Zugangsdaten ein extra Tastaturofeld zu Verfügung stellt. Zusätzlich werden die Eingaben mit einer Domain etikettiert. ScreenPass verwendet diese Etiketten um die Spur der Benutzerdaten zu verfolgen, wie sie sich über die App verbreiten.

4. EFFEKTIVITÄT VON PRÄVENTIONSTECHNIKEN

Es gibt noch weitere Sicherheitssysteme [16] [13] [5]. Um aber effektiv gegen Phishing zu kämpfen muss ein Tool nicht nur Sicherheit gewährleisten, sondern vor allem benutzerfreundlich sein, dass Internetnutzer es auch verwenden. SSL Zertifikate sind eine sichere Methode um sich vor Angriffen zu schützen, auch immer mehr E-Mail Anbieter steigen auf diese Art der Verschlüsselung um. Allerdings werden die Zertifikate immer komplexer und sind für manche Nutzer schwer zu verstehen [13]. Ein weiterer Vorteil ist, dass die meisten entwickelten Sicherheitstools universell verfügbar sind, sodass sie sich jeder Internetnutzer kostenlos herunterladen kann [1]. In den letzten Jahren wurde viel geforscht und man hat sich intensiv mit dem Thema Phishing beschäftigt. Das zeigen die zahlreichen Präventionsmethoden, Paper die darüber geschrieben wurden und die Gründung der APWG⁴ 2003. Das ist eine weltweite Vereinigung, die auf globaler Ebene gegen Internetkriminalität in den Sektoren Industrie, Regierung und Strafverfolgung, kämpft. Die Reduzierung von Phishingangriffen ist trotzdem kompliziert, da die Attacken immer raffinierter werden. Im Gegensatz dazu müssen auch die Präventionsmaßnahmen immer komplexer werden, was zwar Sicherheit gewährleistet, aber viele Benutzer haben Probleme solche Systeme zu verstehen, beziehungsweise Sicherheitsindikatoren richtig zu interpretieren und deshalb werden sie kaum genutzt. Vor allem unerfahrene Internetnutzer schätzen die Gefahr oft falsch ein und haben nicht das Bedürfnis sich zu schützen. Viele gute Tools sind weitgehend unbekannt, weil sich nur wenige mit dem Thema beschäftigen und das richtige Bewusstsein dafür haben [5]. Das ist wohl eins der größten Probleme von Websicherheit, dass es nicht das primäre Ziel von vielen Nutzern ist sich zu schützen [15].

5. SCHLUSSFOLGERUNG

Das Ziel von Phishing ist es, menschliche Schwachstellen im System herauszufinden und auszunutzen, somit ist der Benutzer das schwächste Element in der Sicherheitskette [16]. Dieses Problem ist im Bezug auf die Vielzahl der verschiedenen Angriffsarten breit gefächert und es existiert im Allgemeinen keine perfekte Lösung, da viele Techniken für spezielle Angriffe implementiert werden [4]. Präventionstechniken alleine können das Phishingproblem nicht lösen.

⁴<http://www.antiphishing.org/about-APWG/>, abgerufen am 10.06.2014

Neben der Installation einer guten Sicherheitssoftware, ist es unverzichtbar diese regelmäßig zu aktualisieren, genauso das Betriebssystem. Angebotene Updates sollten baldmöglichst ausgeführt werden. Mit der erforderlichen Sorgfalt kann man das Internet gefahrlos verwenden. Angreifer profitieren von dem gewohnheitsmäßig bedenkenlosen Umgang mit dem Internet vieler Nutzer. Es ist wichtig, dass man seine Handlungen überprüft und sich deren Konsequenzen bewusst ist, da man dazu neigt, eher mit „Ja“ als mit „Nein“ auf eine Nachricht zu antworten. Es sind oft nur kleinen Entscheidungen die verheerende Auswirkungen haben können [3].

6. REFERENCES

- [1] S. Abu-Nimeh, D. Nappa, X. Wang, and S. Nair. A comparison of machine learning techniques for phishing detection. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*, pages 60–69, SMU HACNet Lab Southern Methodist University Dallas, TX 75275, 2007. ACM.
- [2] R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pages 581–590. ACM, 2006.
- [3] A. A. Khan. Preventing phishing attacks using one time password and user machine identification. *International Journal of Computer Applications (0975 887) Volume 68o.3*, 2013.
- [4] M. Khonji, Y. Iraqi, and A. Jones. Phishing detection: A literature survey. *IEEE*, 2013.
- [5] E. Kirda and C. Kruegel. Protecting users against phishing attacks. *The Computer Journal*, 49(5):554–561, 2006.
- [6] M. Landman. Managing smart phone security risks. In *2010 Information Security Curriculum Development Conference*, pages 145–155. ACM, 2010.
- [7] E. Lin, S. Greenberg, E. Trotter, D. Ma, and J. Aycock. Does domain highlighting help people identify phishing sites? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2075–2084. ACM, 2011.
- [8] D. Liu, E. Cuervo, V. Pistol, R. Scudellari, and L. P. Cox. Screenpass: secure password entry on touchscreen devices. In *Proceeding of the 11th annual international conference on Mobile systems, applications, and services*, pages 291–304. ACM, 2013.
- [9] M.-E. Maurer, A. De Luca, and T. Stockinger. Shining chrome: using web browser personas to enhance ssl certificate visualization. In *Human-Computer Interaction-INTERACT 2011*, pages 44–51. Springer, 2011.
- [10] D. Miyamoto, H. Hazeyama, and Y. Kadobayashi. An evaluation of machine learning-based methods for detection of phishing sites. In *Advances in Neuro-Information Processing*, volume Volume 5506, pages 539–546. Springer, 2009.
- [11] J. Mu, A. Cui, and J. Rao. Android mobile security-threats and protection. In *International Conference on Computer, Networks and Communication Engineering (ICCNCE 2013)*. Atlantis Press, Department of Computer Science University of Southern Polytechnic State University, USA, 2013.
- [12] C. Mulliner, R. Borgaonkar, P. Stewin, and J.-P. Seifert. Sms-based one-time passwords: attacks and defense. In *Detection of Intrusions and Malware, and Vulnerability Assessment*, volume Volume 7967, pages 150–159. Springer, 2013.
- [13] S. Y. Na, H. Kim, and D. H. Lee. Prevention schemes against phishing attacks on internet banking systems. *International Journal of Advances in Soft Computing & Its Applications*, 6(1), 2014.
- [14] C. Whittaker, B. Ryner, and M. Nazif. Large-scale automatic classification of phishing pages. In *NDSS*. Google Inc., 2010.
- [15] M. Wu, R. C. Miller, and S. L. Garfinkel. Do security toolbars actually prevent phishing attacks? In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pages 601–610. ACM, 2006.
- [16] C. Yue and H. Wang. Anti-phishing in offense and defense. In *Computer Security Applications Conference, 2008. ACSAC 2008. Annual*, pages 345–354. IEEE, 2008.

Crowdsourcing with Gamification

Fabian Göttl
Universität Passau
Innstr. 43
94032 Passau, Germany
fabian.goettl@stud.uni-passau.de

ABSTRACT

Crowdsourcing is an online, distributed problem-solving model and grants solutions to problems that cannot be computed by machines. Since the introduction of the term "Crowdsourcing" in Jeff How's article "The Rise of Crowdsourcing", created in 2006, the model has emerged during the last few years and has gained popularity among institutions, companies and universities. Amazon's Mechanical Turk is a successful crowdsourcing application, where over 200 000 computation tasks are solved daily by humans. Each day, altogether 40 000 Dollars are paid to contributors as reward for solving tasks. Gamification is an alternative rewarding technique. Instead of money, the player gets rewarded with entertainment, what makes it possible to attract voluntary crowdsourcing participants and to rise their engagement in the platform.

The focus of this paper is the role of gamification in crowdsourcing tasks, rather than crowdsourcing in general.

Keywords

Crowd knowledge, Mechanical Turk, Micro task, Games with purpose

1. INTRODUCTION

Crowdsourcing is a problem-solving model in which a task, commonly solved by workers, is outsourced to a large group of unknown people called the crowd, by means of an open call [1]. The crowd, especially an online community, returns the solutions to the job provider, called crowdsourcer. To improve the engagement of the performers in a platform, the crowdsourcer usually compensates contributors with small amounts of money or other rewards for solving micro tasks (e.g., Amazon Mechanical Turk [2]).

Money is not necessarily the greatest motivation for providing workforce, instead intrinsic motivation is the crucial factor [3]. Intrinsic motivation is a behaviour that is driven by internal rewards like pleasure or feelings to contribute to an important subject. It stands in contrast with extrinsic

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Advances in Embedded Interactive Systems '14 Passau, Germany
Volume 2, Issue 3 (October 2014). ISSN: 2198-9494

motivation that engages a behaviour to gain external rewards like money [4]. Intrinsic motivated users are more likely to engage willingly in a task, hence glory, proud and reputation tend to contribute more than financial compensation. That is the reason why open source projects or other collaborative projects like Yahoo Answers have greater success than their economical equivalents [3].

Human intrinsic behaviour motivates usage of the "Gamification" approach. This term refers to implement gameplay elements and processes in non-gaming applications to incentivize high participation and efforts. Typical gameplay elements are experience points, highscores, achievements and virtual goods [5]. Crowdsourcing work can get "gamified" by adding game mechanics on top of the actual task [6]. This enables crowdsourcing take advantage of a form of intrinsic user behaviour, the so-called "game-like-behaviour": "focus on the task at hand, multitasking under pressure, work overtime without discontented attitude, always keep retrying when fails, etc." [5]

Gamified crowdsourcing applications are also called "Games with a Purpose" (GWAPs) [7]. In general, these are digital games where players generate useful data as a by-product of play [7].

In this work, I investigate common techniques and game mechanics to design GWAPs and show up their opportunities in exemplary applications in science and economy. This part has introduced the terms "Crowdsourcing" and "Gamification" in general. The second part provides their domains and applications. The third and fourth part focuses on design patterns and game mechanics to gamify crowdsourcing tasks, while in the fifth part, techniques to rise player enjoyment are presented. Finally, the sixth part focuses on current gamification frameworks.

2. DOMAINS AND APPLICATIONS

The Games with a Purpose approach used in crowdsourcing terms showed enormous initial potential. The first, and perhaps most successful, game called ESP Game[7] was attracting over 200,000 players. In the game two random players are shown the same picture. The goal is to guess how the partner describes the image and type in that description under time constraints. If the descriptions are matching, the player will be rewarded with score points. These image annotations are useful to train content-based image retrieval tools, because the quality has shown to be as good as expertise image annotations. The game was so successful, that Google bought a license and developed it to Google Image Labeler, which was online from 2006 to 2011 [6].

GWAPs are suitable for many different types of crowdsourced data collections and are applied in areas like information retrieval, multimedia information retrieval and database[6, 8]:

- Image annotations e.g. ESP Game[7], Matchin[9], Magic Bullet[10]
- Audio annotations e.g. Herd It¹, WhaleFM²
- Video annotations e.g. OntoTube[11], Yahoo’s Video-TagGame[12]
- Text annotations e.g. Phrase Detectives³
- improving search results e.g. Microsoft Page Hunt[13]
- biomedical applications e.g. Foldit⁴, Phylo⁵, EteRNA⁶
- digitalization and transcriptions e.g. Ancient Lives⁷, Digitalkoot[14]
- social bookmarking e.g. Collabio[15]

3. CROWDSOURCING DESIGN PATTERNS APPLIED IN GWAPS

In the following section, I present patterns to design crowdsourcing systems with accurate data output and show examples how they are applied with gamification.

Micro-tasks are not always solved correctly, since humans tend to make mistakes or cheat the system selecting random answers for their own profit [5]. Hence a crowd’s judgment is often described as signal with noise. “Averaging judgments will remove the noise and extract the signal” [16]. Accomplishing this requires an evaluation process as inherent part of the crowdsourcing application.

To validate and enrich data, crowdsourcing tasks are split into sub-tasks, which are solved respectively in different processing instances. Later, their output is aggregated to determine a sufficient solution of the main task [17]. Sub-tasks can be represented as logical units [18].

Logical units that introduce users into a creation process are essential to gain initial data output. Possible data creation units are Create/Generate, Find, Improve, Edit, or Fix[18]. Within the first unit, users are able to create or generate any data. Otherwise, new data can also be determined of existing data by applying logical units like Find, Improve, Edit, or Fix.

With quality control units like ”voting up/down to generate a rank”, ”voting for accept/reject” or ”voting for best”, users can validate previously collected data[18].

The following subsections show up exemplary applications, which have implemented logical units in combination.

¹<http://apps.facebook.com/herd-it>

²<http://whale.fm>

³<http://anawiki.essex.ac.uk/phrasetectives/index.php>

⁴<http://fold.it/portal/>

⁵<http://phylo.cs.mcgill.ca/>

⁶<http://eterna.cmu.edu/web/>

⁷<http://ancientlives.org>

3.1 Create-Vote pattern

The “Create-Vote” pattern is frequently used in crowdsourcing applications and consists of splitting the task into two HITs (human intelligence tasks) [18]. In the first HIT, data is created. Users are allowed to insert any data. Later, in the second HIT, other users can vote if the data inserted previously is right or wrong. The vote HIT only allows a Boolean value to be sent and controls the quality of the Creation HIT, whereas redundancy controls the quality of the Voting HIT [18].

This evaluation pattern can be used to precisely recognize optical character recognition (OCR) images by the crowd even if they are in occasional instances very hard to decipher. Commonly, mistakes are inevitable: Typing errors occur or apostrophes are omitted. This technique allows to extract the correct or best answer from the solution space [19].

An example that applies the “Create-Vote” pattern is Digitalkoot[14] by The Finnish Nation Library. The institution digitized their newspaper archives with scanners and had to resolve OCR errors. As government organization, they had limited budget and could not compensate workers assigned to solve OCR errors [14]. Therefore a gamified crowdsourcing application was designed and implemented to use the free workforce of the crowd.

Efforts in fixing bad OCR results were made early by the reCAPTCHA project [19]. CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart) are used to protect websites from automated hits. The user has to enter letters of a distorted image generated by the server. After the dispatch the words are matched. If they do match, access is granted. The main idea of the reCAPTCHA project is to “recycle” this authorization process to fix OCR errors. Therefore it does not generate distorted images. Instead, images of wrongly recognized OCR words have to be deciphered [19].

The Digitalkoot system follows a similar idea but was implemented as a game. It was published at an own website, which included two different gameplay types following the “Create-Vote” pattern:

Create: The aim of the game “Mole bridge” was to build a bridge and save the moles from falling down (see Figure 1). The bridge exists out of blocks. The player has to earn them typing in words that are shown her as OCR image. If the answer is right the block turns to steel, otherwise they explode and destroy neighbouring bridge blocks. With each HIT the player creates data for the second game [14].

Vote: In “Mole hunt” moles are appearing out of five different holes with wooden signs displaying an OCR image and the supposed word recognized by players in previous game or by the computer. The player has to decide if the words are matching by clicking a checkmark or a cross (see Figure 2). If a task is correct, a metaphor like “growing flowers” will be shown. This game mode evaluates the correctness of each word until enough positive validations have been received [14].

3.2 Create-Improve-Compare pattern

The “Create-Improve-Compare” [18] pattern includes two other evaluation techniques. To improve the data collected in the Create HIT, the user is able to change data or add additional information. Second, she is able to compare different suggestions and select the best solution. This technique



Figure 1: Screenshot of the Mole bridge game[20]



Figure 2: Screenshot of the Mole hunt game[20]

reveals its full potential in applications that needs accurate, short, but complete data sets [18]. For example it can be used to paraphrase words, what makes it possible to extract word sense and to build artificial intelligence.

4. GAME MECHANICS

Creating a game with a purpose necessarily requires embedding HITs into a game environment. Developers have to check if a game with game mechanics similar to the task exists. If so, they can integrate the task within the game. Otherwise custom game mechanics have to be implemented [21]. This section lists game mechanics, which are suitable in crowdsourcing contexts and are compiled from the tutorial "Introduction to Games with a Purpose" [21]:

Tile-placement: Place a piece to score points, taking into consideration piece location, group, color and cluster size.

Pattern recognition: Align sequences contained in rows to obtain the greatest number of columns that match in color. Used to arrange DNA, RNA or protein sequences to identify regions of similarity.

Line drawing: Drawing lines in certain ways, e.g. the shapes of an object in an image to make other players guess

the object. Suitable to segment images and to get detailed image information.

Memory: The Player has to recall previous game events or information to reach an objective. For example the visual memory can be exploited to find images, which are similar.

Partnership: Players are able to help each other and build teams, e.g. give her partner hints for guessing a secret word.

Input Agreement: Two players in one game instance get input data, e.g. an audio file, to paraphrase it, while everyone can see the partner's paraphrases. The data is not necessarily the same. Simultaneously each side has to decide, if they have the same input as the partner.

Output Agreement: Players get the same input, but no communication between partners is allowed. The players have to find the opponents answer with multiple trials. Suitable for multiplayer games. E.g. ESP Game[7]

Inversion problem: One player receives input data and has to paraphrase this data. Other players receive his or her textual descriptions, which have to be used as hints to guess the input data.

Prerecorded Games: Used when the amount of players is insufficient. Makes it possible to play the game anytime, but is expensive in implementation: Modeling and storing of game actions, as well as a bootstrapping phase to build an initial data set is costly.

Algorithmic Evolution: Algorithms do not always deliver the best or correct solutions. Human can be used to check the output of an algorithm and correct it if it is wrong. For example, it is used for validating OCR recognition algorithms. Suitable for singleplayer scenarios.

Hybrid approaches: Obtaining a (complex) solution by combining previous approaches and use them in sequence. Results and user-generated content of a game instance can be mapped as input of another instance. [21]

5. INCREASING PLAYER ENJOYMENT

Crowdsourcing applications require a great user base to generate sufficient data. The success of a GWAP depends on attracting this crowd of free workers and motivate them to do persistent precise work.

Like introduced in this paper, gamification is used for this approach, but it necessarily requires a good game design. Providing feedback to users on their work and understanding the motivation of players presents a major challenge. To create a enjoyable game, studying researches in digital games and applying their techniques and suggestions is inevitable. Therefore, two exemplary sources focusing on methods for increasing player enjoyment are introduced in next subsections.

5.1 GameFlow model

In literature, a model was constructed to evaluate player enjoyment in games, called the GameFlow model [22]. It consists of eight core elements: concentration, challenge, skills, control, clear goals, feedback, immersion and social: A enjoyable game has to require concentration, but its player must still be able to concentrate through even a high workload. Furthermore tasks must be sufficiently challenging and the player must be skilled enough to master them. Tutorials or initial levels should teach players how to play the game. Players require clear goals, so that they can complete the tasks.

Feedback methods are able to reveal the progress towards

completing tasks or the quality, how the player has solved them. If the player is adequately skilled and provided with clear goals and immediate feedback, then he or she will feel a sense of control over their actions. This results in a feeling of "total immersion or absorption in the game" [22], which leads player to "lose awareness of everyday life, concern for themselves, and alters their sense of time" [22]. The last core element shows up the social incentive of games. Some people play games to interact with other people, regardless of the task or the game itself [22]. Therefore games should support competition, social interaction and competition between players.

5.2 Game challenges

As mentioned in the GameFlow model, challenge is a key aspect of any successful game. In "Designing Games With a Purpose" [23], von Ahn and Dabbish teaches how to incorporate additional goal-based motivation into GWAP design. This is another approach to increase player enjoyment. Thus, the following section shows up a compilation of von Ahn's game features to introduce challenge in GWAPs:

Timed response makes players to solve tasks under time constraints. If they are able to accomplish a number of problems without reaching a previously specified time limit, they may be given extra points. This method establishes an explicit goal, that might be not trivial for players to achieve. It is essential, that the time limit is chosen wisely to introduce challenge. For providing sufficient feedback, the time remaining and the time limit must always displayed during the game. This game feature is motivated by the fact, that challenging and well-specified goals lead to more contribution than easy and unclear goals [23].

Score keeping motivates players by granting them points as reward for each successful action. The player obtains a performance feedback and can distinguish how much effort, performance and score points leads to a winning condition. Additionally, the feature triggers incentives to beat scores of previous games or completing all tasks within the given time limits [23].

Player skill levels (also called "Ranks") are able to be achieved by players based on the number of points they accumulate. Newcomers to the game start with zero points, hence they are on the lowest skill level. To advance in levels, they have to earn a certain number of points. During the game, the current skill level and the number of points to reach next level are displayed. A data analysis of von Ahn's ESP Game [7] leads to the conclusion, that many players continue playing to just reach a new rank [23].

High-Score lists are lists showing username and corresponding score points of players with highest number of points. The list can be varied in time periods, e.g. year, last month, past hour or all-time. A hourly list incentivizes players to aim to get onto the list and provides quick feedback during this process. Longer time periods define goals of increasing difficulty and motivates players for extended game play [23].

Randomness is effective for keeping the game interesting, even for experienced players. Inputs from a game session are randomly selected from a set of possible inputs, what makes the task difficulty varying. The lack of knowledge if inputs can be completed within time limits adds to the challenge. If players are paired randomly, cheating will be prevented

and each game session will get its own uniqueness [23].

6. GAMIFICATION FRAMEWORKS

To make the development process of gamified applications as fast and easy as possible, open source or proprietary tools and frameworks have been developed. In general, the frameworks are intended for websites and mobile apps. Since GWAPs are able to be published at these platforms, the frameworks are usable for implementing game elements into GWAPs also.

6.1 Commerical products and services

Badgeville⁸ provides relevant tools and a "Dynamic Game Engine" that serves an easy and flexible way to setup behaviours, rewards, missions. The tool "Gamification Widget Studio" offers to design and configure game mechanic widgets. "Social Fabric" integrates a social graph, social notification, and activity streams for better social engagement [24].

Bunchball⁹ provides designers, engineers and marketers a comprehensive set of game elements like points, badges and virtual goods. The platform also includes game actions, group and comment systems and social media embed modules. "Nitro Elements" consists of cloud-based plug and play apps that are aimed for quick implementation of gamification [25].

6.2 Open(source) gamification platforms

UserInfuser¹⁰ is a popular open source project that provides customizable gamification elements to increase user interaction on websites. The framework includes game elements like badging, points, leader boards and live notifications. Additionally, it provides tools to analyse user behaviour [26].

Mozilla's Open Badge¹¹ provides a software infrastructure to make it easy to create and display badges across the web. Shared badges can be issued as recognition for all types, e.g. learning, achievements that take place anywhere, a certification earned or providing a useful technical answer. The badges could be embedded in the personal website or shared at social media platforms [27].

7. CONCLUSIONS

GWAPs are expensive and challenging to develop. In order for GWAPs to reach their potential, designers have to understand what makes them successful and to a fun and engaging experience for players. The paper showed up applied design patterns and game mechanics that can be adapted to gamify human computation tasks. To ensure that these tasks are solved with sufficient quality, GWAPs must include output validation steps. Engaged users are more likely to launch further game sessions and on account of this produce more data. For ongoing game play, users must be motivated by elements like high-scores, player skill levels or randomness. Existing gamification frameworks helps developers to implement these game elements into GWAPs.

⁸<http://badgeville.com>

⁹<http://bunchball.com>

¹⁰<https://code.google.com/p/userinfuser/>

¹¹<http://www.openbadges.org>

8. REFERENCES

- [1] J. Howe. <http://crowdsourcing.typepad.com>. [Published online; accessed 25-May-2014].
- [2] C.-A. Papadopoulou and M. Giaoutzi, "Crowdsourcing as a tool for knowledge acquisition in spatial planning," *Future Internet*, vol. 6, no. 1, pp. 109–125, 2014.
- [3] N. Archak, "Money, glory and cheap talk: Analyzing strategic behavior of contestants in simultaneous crowdsourcing contests on topcoder.com," in *Proceedings of the 19th International Conference on World Wide Web*, WWW '10, (New York, NY, USA), pp. 21–30, ACM, 2010.
- [4] R. M. Ryan and E. L. Deci, "Intrinsic and extrinsic motivations: Classic definitions and new directions," *Contemporary educational psychology*, vol. 25, no. 1, pp. 54–67, 2000.
- [5] Y. Liu, T. Alexandrova, and T. Nakajima, "Gamifying intelligent environments," in *Proceedings of the 2011 international ACM workshop on Ubiquitous meta user interfaces*, pp. 7–12, ACM, 2011.
- [6] J. Chamberlain, K. Fort, U. Kruschwitz, M. Lafourcade, and M. Poesio, "Using games to create language resources: Successes and limitations of the approach," in *The People's Web Meets NLP* (I. Gurevych and J. Kim, eds.), Theory and Applications of Natural Language Processing, pp. 3–44, Springer Berlin Heidelberg, 2013.
- [7] L. Von Ahn, "Games with a purpose," *Computer*, vol. 39, no. 6, pp. 92–94, 2006.
- [8] A. Bozzon and L. Galli, "An introduction to human computation and games with a purpose," in *Proceedings of the 13th International Conference on Web Engineering*, ICWE'13, (Berlin, Heidelberg), pp. 514–517, Springer-Verlag, 2013.
- [9] S. Hacker and L. Von Ahn, "Matchin: eliciting user preferences with an online game," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 1207–1216, ACM, 2009.
- [10] J. Yan and S.-Y. Yu, "Magic bullet: A dual-purpose computer game," in *Proceedings of the ACM SIGKDD Workshop on Human Computation*, HCOMP '09, (New York, NY, USA), pp. 32–33, ACM, 2009.
- [11] K. Siorpaes and M. Hepp, "Games with a purpose for the semantic web," *IEEE Intelligent Systems*, vol. 23, no. 3, pp. 50–60, 2008.
- [12] R. Van Zwol, "Video tag game," Nov. 15 2007. US Patent App. 11/941,038.
- [13] H. Ma, R. Chandrasekar, C. Quirk, and A. Gupta, "Page hunt: Improving search engines using human computation games," in *Proceedings of the 32Nd International ACM SIGIR Conference on Research and Development in Information Retrieval*, SIGIR '09, (New York, NY, USA), pp. 746–747, ACM, 2009.
- [14] O. Chrons and S. Sundell, "Digitalkoot: Making Old Archives Accessible Using Crowdsourcing," in *HCOMP 2011: 3rd Human Computation Workshop*, 2011.
- [15] M. Bernstein, D. Tan, G. Smith, M. Czerwinski, and E. Horvitz, "Collabio: a game for annotating people within social networks," in *Proceedings of the 22nd annual ACM symposium on User interface software and technology*, pp. 97–100, ACM, 2009.
- [16] C. G. Harris, "The beauty contest revisited: Measuring consensus rankings of relevance using a game," in *Proceedings of the First International Workshop on Gamification for Information Retrieval*, GamifIR '14, (New York, NY, USA), pp. 17–21, ACM, 2014.
- [17] J. Howe, *Crowdsourcing: Why the Power of the Crowd Is Driving the Future of Business*. New York, NY, USA: Crown Publishing Group, 1 ed., 2008.
- [18] A. Bozzon and L. Galli, "An introduction to human computation and games with a purpose." Link to tutorial slides of the first part: <http://de.slideshare.net/aleboz/an-introduction-to-human-computation-and-games-with-a-purpose-part-i>, 2013. [Published online; accessed 25-May-2014].
- [19] L. Von Ahn, B. Maurer, C. McMillen, D. Abraham, and M. Blum, "recaptcha: Human-based character recognition via web security measures," *Science*, vol. 321, no. 5895, pp. 1465–1468, 2008.
- [20] Website: <http://scistarter.com/blog/2011/03/digitalkoot-an-online-game-for-indexing-finnish-newspapers>. [Published online; accessed 25-May-2014].
- [21] A. Bozzon and L. Galli, "An introduction to human computation and games with a purpose." Link to tutorial slides of the second part: <http://de.slideshare.net/CUBRIKproject/cubrik-tutorial-at-icwe-2013-part-2-introduction-to-games-with-a-purpose>, 2013. [Published online; accessed 25-May-2014].
- [22] P. Sweetser and P. Wyeth, "Gameflow: a model for evaluating player enjoyment in games," *Computers in Entertainment (CIE)*, vol. 3, no. 3, pp. 3–3, 2005.
- [23] L. Von Ahn and L. Dabbish, "Designing games with a purpose," *Communications of the ACM*, vol. 51, no. 8, pp. 58–67, 2008.
- [24] Website: <http://badgeville.com/products>. [Published online; accessed 25-May-2014].
- [25] Website: <http://www.bunchball.com/products/nitro>. [Published online; accessed 25-May-2014].
- [26] Website: <https://code.google.com/p/userinfuser/>. [Published online; accessed 25-May-2014].
- [27] Website: <http://www.openbadges.org/>. [Published online; accessed 25-May-2014].

Usable Security

Jakob Kasbauer
Universität Passau Innstr. 43
94032 Passau, Germany
kasbauej@fim.uni-passau.de

ABSTRACT

Since many designers think that usability and security cannot be achieved at the same time, it is important to provide guidelines and usability studies to evaluate different approaches. In this paper several researches targeting both usable and secure solutions to real world problems are presented. Starting with generic design guidelines and their use on the analysis of a once very popular file sharing program.

Afterwards the usability and security aspects of Out-Of-Band channels in device pairing will be presented by analysing two comprehensive user studies.

At the end I present several usable solutions to current security flaws in smartphone authentication methods.

Keywords

Security, Usability, Guidelines, Out-of-Band, Authentication, Smudge Attack, Shoulder Surfing

1. INTRODUCTION

The term security is often related to software errors like buffer overruns or race conditions and much attention is used on writing correct software implementations. However less effort is spent on providing usable interfaces to guide users through the complex setup and operation of security appliances. As the configuration and operation of such systems are done manually their success heavily depends on the information conveyed by the user interface. Problems in usability often lead to attack vectors which could be easily prevented [22].

The origin of secure computer systems and encryption is in the governmental and military sector where selected people are trained to precisely execute their given orders in conformance to detailed rules. These specialists are able to operate their systems no matter how complex or error prone the user interface is.

The limited number of possible users reduces the urge to create usable and secure interfaces. This established a culture of security appliances with complex user interfaces

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

*Advances in Embedded Interactive Systems '14 Passau, Germany
Volume 2, Issue 3 (October 2014). ISSN: 2198-9494*

and taught users that secure software is often hard to use. [23]

2. KA-PING YEE'S DESIGN GUIDELINES

To improve security, predictability, reliability and usability Yee created a set of principles as an aid for designing user interaction systems. The rules were created in a way that a violation of one criterion would lead to a security vulnerability. Therefore, to achieve full security coverage the rules do overlap to some extent.

In contrast to previous security guidelines the next recommendations are more focused on user interfaces and user experience.

The following is an updated list from Yee's website. [21]

- **Path of least resistance.** Match the most comfortable way to do tasks with the least granting of authority.
- **Active authorization.** Grant authority to others in accordance with user actions indicating consent.
- **Revocability.** Offer the user ways to reduce others' authority to access the user's resources.
- **Visibility.** Maintain accurate awareness of others' authority as relevant to user decisions.
- **Self-awareness.** Maintain accurate awareness of the user's own authority to access resources.
- **Trusted path.** Protect the user's channels to agents that manipulate authority on the user's behalf.
- **Expressiveness.** Enable the user to express safe security policies in terms that fit the user's task.
- **Relevant boundaries.** Draw distinctions among objects and actions along boundaries relevant to the task.
- **Identifiability.** Present objects and actions using distinguishable, truthful appearances.
- **Foresight.** Indicate clearly the consequences of decisions that the user is expected to make.

3. USABILITY AND PRIVACY: A STUDY OF KAZAA P2P FILE-SHARING

KaZaA was the most used P2P file sharing system after the shut down of Napster. It was mainly used for sharing

multimedia files. KaZaA attracted a wide range of users and was very popular. Thus many novice computer users operated the application without an exact understanding of its behaviour.

KazaA enabled users to download and upload files in a default folder. Moreover it also allowed users to share additional folders. Because many novice users had problems with understanding the hierarchical structure of file systems and due to misleading naming of KazaA's folders, in many cases the C: drive and thus all its subfolders were accessible for outside parties.

Although KazaA was not designed as a security program like PGP¹ it failed many aspects of Yee's Guidelines. This resulted in leakage of sensitive data. Not only for the KazaA user but also for every other user of this computer. For example if there is one computer per family and one family member installs KazaA then the files of other users are made public and thus mitigating all security measurements installed by other users.

The accessibility of private files was verified by searching for email inbox folders, databases and private spreadsheet files on the KaZaA network. Good and Krekelberg were able to find 156 distinct users sharing the file inbox.dbx over a period of 12 hours [8].

Furthermore to prove that sensible files are downloaded by malicious agents they set up a honeypot installation, sharing files with appealing filenames such as Inbox.dbx and Credit Cards.xls. They detected 8 downloads in 24 hours on their honeypot installation.

In an additional user study Good and Krekelberg shared all files on the hard drive and only 2 out of 12 users were able to correctly tell that all files and folders were shared [8].

Payne and Edwards stated that :

...it seems likely that Kazaa's problems could be fixed through interface changes alone. [14]

The lessons learned from this study are also applicable to a wide range of other file sharing programs and cloud synchronization tools. Those programs also have the need to configure the shared folders and inform the user of their recursive folder sharing behaviour.

Failed Rules of Yee's Guideline

Because a variety of settings control the access to files and folders, the interface fails *Active authorization*, *Visibility* and *Foresight*. Due to the implicit sharing of subfolders KazaA isn't *Expressive* about the shared files and folders.

4. OUT-OF-BAND CHANNELS IN DEVICE PAIRING

Securely bootstrapping ad-hoc connections is a rising need with the increasing number of wireless enabled gadgets like smartphones and the Internet of Things². Establishing secure wireless connections is also relevant with the growing number of radio communication technologies like Bluetooth, NFC, WiFi and ZigBee. Along the near ubiquity of devices with wireless communication it is important to provide an

¹Pretty Good Privacy, a computer program for encryption, decryption and authentication

²Internet of Things, the interconnection of many embedded devices via the existing Internet infrastructure

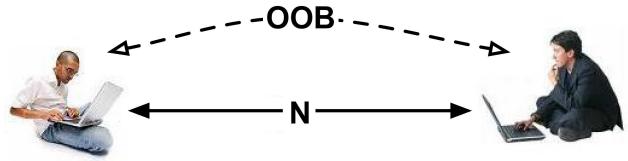


Figure 1: Graphical representation of Out-Of-Band Channel. N is the standard wireless channel that is vulnerable to Man-In-The-Middle attacks. [10]

easy to use yet secure method to establish an ad-hoc connection without the need of a public key infrastructure or trusted third parties since these devices often hold private or financial data or are used in two-factor authentication systems.

The term *Out-Of-Band* describes the means of data transmission outside the main communication channel. The *Band* refers to the electric frequency-band, where a band is a small section of radio frequencies.

With this additional channel it is possible to securely establish an exchange of public keys. Afterwards an RSA encrypted transfer channel can be achieved. Without this additional channel a user could not detect a possible Man-In-The-Middle³ attack or a rogue WiFi access point.

The Out-Of-Band channel is a human perceivable medium like audio or displayed text. A human operated Out-Of-Band channel is usually of very low bandwidth due to the limited possibilities of human sensing or due to lacking input means on the devices. E.g. a smartphone with a small on-screen keyboard, or a Bluetooth headset with a limited number of pushbuttons.

Since this medium is like a face-to-face conversation, an attacker could overhear the transmitted data but could not modify or delete transmissions. So this medium is authentic and data integrity is ensured but not secret.

The channel N stands for the normal wireless medium that is used for exchanging the public keys and for transmitting the payload data after bootstrapping the encryption. N is a high-bandwidth, non-human-perceivable medium like WiFi or Bluetooth. Since a possible attacker could wire-tap this medium and therefore intercept or modify the transferred data, N is usually prone to Man-In-The-Middle attacks or Evil-Twin attacks.

After the initial key exchange via the normal wireless channel the hashes of the public keys are transferred over the Out-Of-Band channel where the user has to check the correctness of the hashvalues. Previous research has studied the minimum bitlength for preventing hash-collisions and the results range from 16 bits [13] to 68 bits [12]. There is a multitude of available algorithms for this protocol for example *Symmetrised Hash Commitment Before Knowledge* (SHCBK) [13] or *Short Authenticated String* (SAS) or *MANA* [7]. The purpose of SAS and MANA is to reduce the number of required bits over the Out-of-Band channel.

³Man-In-The-Middle, an attack where the transfer medium is wire tapped and the attacker relays every message. The attacker is able to modify and eavesdrop all exchanged data.

One example is the pairing of legacy⁴ Bluetooth devices. An initial alphanumeric Personal-Identification-Number (PIN) is set on one device and the same PIN must be entered on the other Bluetooth devices that are willing to communicate. Nevertheless this pairing method is prone to the attacks shown in the works of Shaked and Wool [17] and Jakobson and Wetzel [9].

Another well known application is the Wi-Fi Protected Setup (WPS) method. The Out-of-Band channel is implemented by PIN, NFC, USB or by pushbuttons on both devices. However this method is also vulnerable [18].

Since both mentioned pairing methods are vulnerable to attacks, the need for a secure implementation of Out-Of-Band authentication is high. Furthermore smartphones with their multitude of sensors provide many possibilities to implement the second band.

User Studies

The first comprehensive user study for comparing Out-of-Band channels was done by Uzun et al [11]. Another extensive user study was conducted by Kainda et al. [10]

User study by Uzun et al.

Uzun et al. examined a wide range of methods, including infrared, comparison of images, blinking lights, sound patterns, pushbuttons, accelerometers and text input methods like copy-and-confirm or choose-and-enter.

Uzun et al. state that number-comparison is the overall winner in terms of usability scores. It is also more resilient to safe errors compared to image-comparison or phrase-comparison. Furthermore number-comparison is easy to implement since it only requires a small display capable of showing few numeric digits.

Audio pairing is the favoured method if one device lacks a display but has a microphone and the other device contains a speaker, for example pairing smartphones with Bluettooth Headsets.

On input constrained devices, like pagers and WiFi access points, Vibrate-Button is the best method followed by LED-Button and Button-Button.

User Study by Kainda et al.

In this study the methods were grouped as followed: *Compare & Confirm* (C&C), *Compare & Select* and *Copy & Enter* (C&E). The user compared following data representation types : strings, sounds, melodies and images. The user was asked to compare data in following test forms: two identical data, significant different data, and data that was nearly identical and only differed in one single character. In an additional method the user had to take a picture of a barcode, that was displayed on the other device.

Kainda et al. examined the sole usability of methods and also the usability in respect to critical security error probability.

The most usable methods are : Numeric C&C, Alphanumeric C&C, and Words C&C.

The most usable and secure methods are : Numeric C&E, Alphanumeric C&E and Barcode.

This study revealed that comparing melodies is not usable since many probands stated that "not being a musician" renders this task very hard. Melodies also have the

⁴prior to Bluetooth 2.1

problem that the user has to pay close attention resulting in low usability. Furthermore an interruption or external noise requires to restart the listening process. The same problems apply to the methods numeric & sound and alphanumeric & sound.

Furthermore users reported that digits or characters are easier to compare than long sequences of words or word-phrases.

67% of the users older than 45 had problems with the barcode method. They stated that it was not clear how to take the photo and how sharp it has to be.

Concerning the critical security failures and usability, the method *Compare & Enter* achieved the highest scores. The participants stated that they had the possibility to double-check their inputs. Furthermore this approach forced the users to pay attention. Therefore a user in a rush can not bypass this method by choosing randomly. Users are also quite familiar with the input process since people are used to enter a numeric PIN on payment terminals or type SMS on cell phones.

Despite being very error resistant, the barcode method ranked third because of low usability scores as the participants were unfamiliar with this approach. Kainda stated the barcode method will be more accepted if users are educated or exposed to this technology. The barcode also has the potential to carry more bits of information than human operated text input.

Kainda emphasized that *Copy & Enter* is preferred over *Compare & Confirm* despite that *Copy & Enter* ranked below *Compare & Confirm* in usability scores. Because C&E is not prone to critical security errors and users can not bypass it.

5. SMARTPHONE AUTHENTICATION

"User authentication is one of the oldest and most heavily studied topics in usable security. [14]"

To authenticate a user the verification of one or more factors is necessary. The authentication factors are :

- something the user knows (passwords, PINs)
- something the user has (security tokens, smart cards)
- something the user is (physiological or behavioural characteristics)

Smartphones are able to measure more behavioural and biometric patterns than a common desktop computer because smartphones contain a multitude of sensors like accelerometers, cameras and sometimes fingerprint readers.

However research has shown that not all biometric characteristics are suitable as an authentication factor. Moreover there are many privacy concerns about the use of biometrics. [15]

Since smartphones are liable for theft and often hold sensitive data such as emails and address books the need for secure authentication methods is high. On the other hand most smartphone interactions are very short, for example checking for new email, therefore authentication mechanisms must be easy to use and fast.

5.1 Explicit Authentication

Graphical passwords provide a more usable alternative to alphanumeric passwords and are well suited for touch screen input. As a result Google implemented visual password methods in Android in 2010.

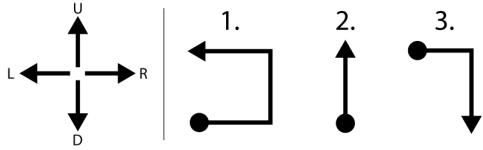


Figure 2: Back-Of-Device authentication shapes. Easier to perform on the backside than Android grid unlock. [5]

Graphical passwords on touch enabled devices provide two major benefits. Firstly users are more likely to remember visual passwords, compared to a password in written word form. Since graphical passwords utilize the picture-superiority effect. Secondly the input of passwords on a touch screen is done "by hand". This leads to additional memorability due to the involvement of the motor memory [20].

However the password input on a touch screen leads to the following attack vectors: Firstly an attacker near to the user can observe the password input and obtain the password. This attack is called shoulder surfing and can be done by spying over the users shoulder or by video recording the user. This vulnerability is critical since smartphone authentication often occurs in public and crowded places. [4]

Secondly fingers leave oily residues on the touch screen surface. The smudge traces from previous logins allow an attacker to (partially) recover the used password. Under suited lighting and camera orientation the smudge traces can be photographed even after placing the phone into a jeans or jacket [1].

The default authentication method on Android is called grid unlock and consists of an oriented drawing between points on a grid.

Back-Of-Device Authentication

Capacitive sensitive areas on the backside of devices were introduced to solve the "fat-finger" problem where the users finger conceals the touch screen during interaction. Placing the area of interaction and the fingers on the backside restores a clear sight of the display. [2, 5]

De Luca et al. proposed to use the backside for password input [5]. This renders the authentication more resilient against by-standing shoulder surfers. Since a smartphone is usually not held vertically but slightly tilted, an attacker would have to kneel down in front of the user to get vision of the backside. Kneeling down or other unusual posture would raise suspicion. Furthermore camera attacks are less likely to be successful because the camera would have to face upwards and be positioned on the floor.

The standard Android grid unlock method is not usable on the backside because users are not likely to hit the spots of the grid without seeing them. Therefore De Luca et al. proposed the use of special Back-of-Device shapes. [5] These shapes consist of 3 consecutive drawings, where each drawing is composed of Up/Down/Left/Right strokes. This input method does not require absolute finger precision and relies on easier relative movements.

In addition to the resilience against shoulder surfing, the Back-Of-Device shapes are resilient to smudge attacks because the drawings are often performed in the same location.

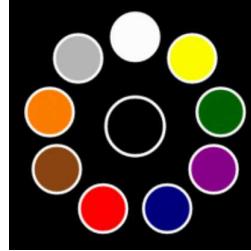


Figure 3: Marbles authentication method. [19]

The overlapping smudge traces make it difficult for an attacker to recover the used shapes.

As an improvement over the Back-of-Device input, De Luca et al. developed an authentication mechanism that makes use of both sides, allowing a user to switch the used surface ad-hoc, called XSide. [4] When threatened by an shoulder surfer the user is able to use the side that is opposite to the attacker and perform the strokes on the secure side.

In the user studies Back-Of-Device and XSide produced more critical errors and were slower than Android grid unlock but were also significantly more resilient against shoulder surfing. However the major drawback of this method is the need for additional capacitive sensor hardware.

Making Graphic-Based Authentication Secure against Smudge Attacks

Von Zezschwitz et al. proposed several novel graphical authentication methods that were designed to be resistant against smudge attacks. [19]

The resistance is achieved by randomizing the order of the input tokens, by blurring the smudge trails within one authentication and by rotating the view port.

The most promising approach is the *Marbles* method and its deviations. Where the password consists of a sequence of colors, represented as marbles. To authenticate the user has to drag the marbles into the inner circle in the right order. The marbles in the outer ring are randomly placed upon each password input.

In the user study by Von Zezschwitz et al. the marble based methods achieved low error rates and high usability and memorability scores. Furthermore they were very resilient against smudge attacks. With 0% recovery rate in 192 attacks with photographs of the smudge trails. However the login time increased fivefold compared to Android grid unlock.

SmudgeSafe : Image Transformations

This input method proposed by Schneegass et al. maps the touch sensitive area onto a background image. After geometric transformations of the background image the leftover smudge trails do not match any more. Since the geometric transformations are independent of the input method, SmudgeSafe can be applied to a wide range of patterns (like PIN, grid unlock, PassPoints, etc.) and to a wide range of touch enabled devices. Moreover this approach can be implemented in the operating system layer to be used by other authentication applications.

Schneegass et al. conducted a user study and found that



Figure 4: SmudgeSafe, preventing smudge attacks by geometric transformations of the background image [16].

this approach preserves the low authentication time of grid based methods. Furthermore it was significantly more resilient against smudge attacks compared to grid unlock or PIN. However approaches based on the *Marble* method were more resilient against smudge attacks than graphical passwords with transformations.

5.2 Implicit Authentication

Another promising approach are authentication methods based on implicit data input. Since these methods produce high error rates they are not suited for the main authentication but can provide an additional layer of defence or extend the time between explicit authentications. Previous research was focused on the characteristics of the human gait or on key stroke patterns but there are newer approaches based on the characteristics of touch screen input, such as speed, pressure and path of the finger interaction.

Since implicit methods rely on static classifiers or neural networks, the CPU and power consumption is rather high. Furthermore the need for constant data recording in the background prevents the device from going into deeper sleep states, thus resulting in lower battery life [3, 6].

6. REFERENCES

- [1] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith. Smudge attacks on smartphone touch screens. *WOOT*, 10:1–7, 2010.
- [2] P. Baudisch and G. Chu. Back-of-device interaction allows creating very small touch devices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1923–1932. ACM, 2009.
- [3] A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann. Touch me once and i know it's you!: implicit authentication based on touch screen patterns. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 987–996. ACM, 2012.
- [4] A. De Luca, M. Harbach, E. von Zezschwitz, M.-E. Maurer, B. E. Slawik, H. Hussmann, and M. Smith. Now you see me, now you don't: Protecting smartphone authentication from shoulder surfers. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, pages 2937–2946, New York, NY, USA, 2014. ACM.
- [5] A. De Luca, E. Von Zezschwitz, N. D. H. Nguyen, M.-E. Maurer, E. Rubegni, M. P. Scipioni, and M. Langheinrich. Back-of-device authentication on smartphones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2389–2398. ACM, 2013.
- [6] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *Information Forensics and Security, IEEE Transactions on*, 8(1):136–148, 2013.
- [7] C. Gehrman, C. J. Mitchell, and K. Nyberg. Manual authentication for wireless devices. *RSA Cryptobytes*, 7(1):29–37, 2004.
- [8] N. S. Good and A. Krekelberg. Usability and privacy: a study of kazaa p2p file-sharing. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 137–144. ACM, 2003.
- [9] M. Jakobsson and S. Wetzel. Security weaknesses in bluetooth. In *Topics in Cryptology — CT-RSA 2001*, pages 176–191. Springer, 2001.
- [10] R. Kainda, I. Flechais, and A. Roscoe. Usability and security of out-of-band channels in secure device pairing protocols. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, page 11. ACM, 2009.
- [11] A. Kumar, N. Saxena, G. Tsudik, and E. Uzun. A comparative study of secure device pairing methods. *Pervasive and Mobile Computing*, 5(6):734–749, 2009.
- [12] J. M. McCune, A. Perrig, and M. K. Reiter. Seeing-is-believing: Using camera phones for human-verifiable authentication. In *Security and privacy, 2005 IEEE symposium on*, pages 110–124. IEEE, 2005.
- [13] L. H. Nguyen and A. Roscoe. Efficient group authentication protocol based on human interaction. In *Proceedings of Workshop on Foundation of Computer Security and Automated Reasoning Protocol Security Analysis*, pages 9–31, 2006.
- [14] B. D. Payne and W. K. Edwards. A brief introduction to usable security. *Internet Computing, IEEE*, 12(3):13–21, 2008.
- [15] S. Prabhakar, S. Pankanti, and A. K. Jain. Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy*, 1(2):33–42, 2003.
- [16] S. Schneegass, F. Steinle, A. Bulling, F. Alt, and A. Schmidt. Smudgesafe: Geometric image transformations for smudge-resistant user authentication. ACM, 2014. to appear in Proceedings of UbiComp 2014.
- [17] Y. Shaked and A. Wool. Cracking the bluetooth pin. In *Proceedings of the 3rd international conference on Mobile systems, applications, and services*, pages 39–50. ACM, 2005.
- [18] S. Viehböck. Brute forcing wi-fi protected setup. *Wi-Fi Protected Setup*, 2011.

- [19] E. Von Zezschwitz, A. Koslow, A. De Luca, and H. Hussmann. Making graphic-based authentication secure against smudge attacks. In *Proceedings of the 2013 international conference on Intelligent user interfaces*, pages 277–286. ACM, 2013.
- [20] R. Weiss and A. De Luca. Passshapes: utilizing stroke based authentication to increase password memorability. In *Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges*, pages 383–392. ACM, 2008.
- [21] K.-P. Yee. Secure interaction design.
"<https://web.archive.org/web/20120127051714/>
<http://people.ischool.berkeley.edu/~ping/sid/>",
2001. "[last accessed 20-Jun-2014]".
- [22] K.-P. Yee. *User interaction design for secure systems*. Springer, 2002.
- [23] M. E. Zurko and R. T. Simon. User-centered security. In *Proceedings of the 1996 workshop on New security paradigms*, pages 27–33. ACM, 1996.

Challenges in Crowd Monitoring

Aaron Kopp
Universität Passau
94032 Passau, Germany
koppaaro@stud.uni-passau.de

ABSTRACT

This paper gives an overview about crowd monitoring and its challenges. Crowd monitoring plays a serious role wherever big assemblages of people take place. The main question at this is where are especially many people at the same time. That many people at the same place at the same time represent a big safety hazard is well known. An approach to prevent huge stampedes in future is crowd monitoring. The management of the crowd is related to techniques that are developed to monitor and maintain the public order. There are several problems to deal with, using crowd monitoring. In this paper these problems are specified and solutions are given. Also applications and other real uses are presented. Further privacy plays a big role in crowd monitoring and is acquired in this writing.

Keywords

Data mining, Big data, Crowd monitoring, Privacy issues

1. INTRODUCTION

Large concentrations of people, occur frequently in modern society. A major sporting or entertainment event can attract huge concentrations of people. Such large assemblages of people occur usually without serious problems. Occasionally the combination of inadequate facilities and deficient crowd management results in injury and death. The disaster in Duisburg, the love-parade festival, for example was one of the most tragic. 21 visitors died and further 541 were injured. To avert such disasters in future new techniques have to be developed.

Today internet-connected and sensor-equipped portable devices are widely spread. This allows new applications which exploit the opportunities of such devices facilitate to manage crowds. This technique of crowd monitoring is called crowd sensing [2]. The latter is not the only possibility the check crowd behaviour. There are also other options, like video monitoring. Classical observation cameras are widely spread. Although they can mirror recorded

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Advances in Embedded Interactive Systems '14 Passau, Germany
Volume 2, Issue 3 (October 2014). ISSN: 2198-9494



Figure 1: A Thermal image of some people moving in Haram Area [1].

data one on one, an expert is needed, who can estimate the collected data based on the situation. New crowd monitoring techniques which nearly replace this human factor are in development.

2. MAIN TECHNIQUES

Human observers of crowds can detect many crowd features quite easily. They can also estimate in a qualitative way the crowd density. Techniques which replace humans in that context are nowadays rather unrealistic. But they can support them in diverse ways. The two most important and advanced methods to monitor the crowds are presented in this paper.

2.1 Video monitoring

One of the most effective methods to monitor the crowd is video monitoring. Thereby only counting people becomes inefficient when it is required in real-time and when the crowd is dense [1]. Advanced technologies are needed, like infrared thermal video. Here the effect, that individual people as well as a whole crowd generates heat, is exploited. This heat originates from the usually cold environment. This effect is captured by special cameras and is processed with special computer algorithms [1]. This paper will not explain any further details about all the special techniques, because this would be too comprehensive. This method works also in hot

areas, where the surroundings are warmer than the crowd, as seen in figure 1. The colder crowd emphasizes obvious from the hotter ground. The disadvantage of this method is, that it only works reliable, when the environment and the crowd have a bigger gap between their temperatures.

Another method of crowd monitoring with video analytic is to use image processing [3]. Here, the difference between a "naked" ground and a ground with people on it is measured. The edges of single humans are plotted, which allows also to count how many people are on this marked-out area at a certain time. But this method has also its pitfalls. If people carry umbrellas, they cannot be identified as humans, so you have always an error rate to deal with. For example, on raining days, where the most of the people carry umbrellas, this method of crowd monitoring is nearly useless.

2.2 Crowd monitoring via smart-phone

To alleviate the disadvantages mentioned above, researchers took a novel approach by monitoring crowds with their smart-phones. The wishful thinking would be a "sensor-enabled mobile system to assist organizers and participants of public events in emergencies and evacuation situations using human computing principles" [4]. To realize such a system, special applications are needed, which you have to download, if you are participant of an event for example.



Figure 2: Mockup illustration of how such a service could look like on a mobile device during an evacuation situation. It indicates relevant information about danger zones and target area to go to and zones to avoid e.g. due to jamming[4].

Figure 2 shows how such an application could look like. It indicates relevant information about danger zones and tells the user to avoid them. Also it shows safety areas to go to and other zones to avoid for example due to jamming[4]. Every single mobile device could send its information to a centre, which can process the captured data to monitor the crowd. Also danger situations or other important information can be shown in the app.

3. CHALLENGES

This paper should above all give an overview about the challenges in crowd monitoring. There are bunch of problems you have to deal with, when you perform crowd monitoring. On the one side there are technical problems as well

as problems caused by humans, whereby second ones are definitely more complex.

3.1 Technical challenges

20 years ago the principle of crowd monitoring was inconceivable, because the technology that's needed wasn't invented yet. Nowadays most of them are invented or implemented nearly perfect for the use of crowd monitoring. This doesn't mean, that there are no technical problems. They are present, but more in detail. Two of them are expounded in the next paragraphs, big data and data mining.

3.1.1 Big data

Big data, what is big data? It's a term that has been used in the sciences refer to data sets large enough to require supercomputers, although now vast sets of data can be analysed on desktop computers with standard software[5]. Crowd monitoring causes massive sizes of data. For example when you monitor the crowd via smart-phone applications at a huge soccer game, with 50000 visitors , every single device sends a certain amount of data. All together summarize to big data you have to deal with. A wide variety of techniques and technologies has been developed and adapted to aggregate, manipulate, analyse, and visualize big data [6]. Crowd monitoring requires analysing of big data in real-time, because the visitors or citizens have to be informed about safety risks immediately.

3.1.2 Data mining

Data mining is the most important part to deal with handling with big data. Data mining is a set of techniques to extract the most important information from large data-sets, which can't be treated manually by combining methods from statistics and machine learning with database management [6]. Various of the applied procedures descend from statistic and are only adjusted for data mining, what causes a lack of precision. Despite all that for the process of data mining the advantage in run time speed is more important than precision [7].

Data mining entails several problems. The most frequent issue is that parts of the gathered data are either broken or incomplete. These problems are often statistic ones and have to be solved already during the data capture. A second one is the evaluation of data. Evaluation is a very important part in data mining, because otherwise too many unusable information wouldn't be filtered [7]. There are two different methods of evaluation in data mining, Hold-Out and Cross-Validation. This paper won't give more details about evaluation. More details about these two methods and evaluation in data mining can be found in the article *Beating the Hold-out: Bounds for K-fold and Progressive Cross-validation* [8].

Another problem states in interpretation. Statistic algorithms analyses the data without knowing it's meaning. This has superior privacy issues. Therefore they can only process simple models like groups or midpoints. Often the results are no longer comprehensible, but they have to be workable, otherwise the results are not suitable [7].

3.2 Human-induced challenges

The way more complex problems in crowd monitoring are caused by humans. Humans issue a challenge to all monitoring techniques. As mentioned before in the section video-monitoring, it is for example very difficult to count and ob-

serve the behaviour of people by video monitoring when they carry umbrellas. Also crowd monitoring via smart-phone applications doesn't work, if the users handle the application the wrong way. So that users don't prevent crowd monitoring they have to be instructed in the respective method. Another important point is, why should humans support crowd monitoring. They need incentives. How users can be instructed and give them the needed incentives is acquired in the following sections.

3.2.1 Instruction

Instruction of the users means mainly showing them how crowd monitoring works and how they can support it. Let's assume that crowd monitoring is divided in two parts. Monitoring in every day life and monitoring at events or other similar environments. In every day life this can for example happen by presenting the users new techniques in terms of omnipresent mediums, like television. At events people can be briefed about it by printing informations about monitoring on the tickets or installing signs everywhere, where the users can inform themselves.

3.2.2 Incentives

The main question in this section is, how you can motivate people to support crowd monitoring. This is very important, because if the people don't agree with the concept of crowd monitoring, most techniques fail. An good approach would be to point out the advantages of crowd monitoring to the user. If there are doubts about crowd monitoring it is possibly a good way to eradicate them. Another approach could be to combine voluntary crowd monitoring with gamification. For example design the smart phone application, that is used for crowd monitoring, as game. As an expiring example techniques from the field crowdsourcing, where gamification is already implemented, could be used [14].

4. APPLICATIONS AND DOMAINS

Being still in the initial stages of development, crowd monitoring has been realised frequently at major events and in case of researching processes. Three of them are presented in this paper.

4.1 City police

To prevent dangerous situations in case of huge assemblies of peoples, the "DFKI", the german research center for artificial intelligence, developed an smart-phone application for the Olympic games in London 2012. The application serves the information exchange between the london police and the citizen and visitors. Based on the integrated crowd monitoring technique, crowd movements can be followed in real-time and people can be informed with safety relevant information. The application called *city police* informs about the direction, the size and the velocity of the crowds.

For example if there is an gathering at the subway station registered by the app, the users are informed immediately about another close by station via push message. This technology has been developed by the EU-project "SOCIONICAL", where research centres and tertiary institutions examine how technology and social interaction work together. Prof. Dr. Paul Lukowicz and his team accomplished the development work. One issue particular attention has been given is the aspect of data protection. The use of the application is voluntary and the users are completely anonymous.



Figure 3: Extract of the city police application.

Further every single person can choose which informations are transmitted [11]. Figure 3 shows an extract of the city police application. Additional to the crowd monitoring aspect, the app also presents the user helpful informations like maps, police stations, pharmacies, hospitals and similar institutions. Also the app has an implemented service, where the user can contact the police immediately. The police can also contact all smart-phones if they need information, for example how the traffic state.

4.2 "CCTV"

CCTV or Closed Circuit Television label video cameras are applied to monitor public or private spaces, the traffic and technical institutions. CCTV cameras are nowadays nearly everywhere, for example in supermarkets, gas-stations, public places and even at home. Although CCTV isn't equatable to crowd monitoring, it provides the basis for many crowd monitoring techniques [12]. From the pictures a standard CCTV camera records, relevant informations for monitoring can be extracted and be processed [3]. One method which utilizes CCTV recorded information is the method crowd monitoring using image processing, which is described in the section *Video monitoring*. Using CCTV does only partially conforms nowadays standards, because it is an comparatively old technique. The first CCTV cameras were introduced 1942 [15].

4.3 Crowd monitoring via Bluetooth

In the paper *Collaborative Crowd Density Estimation with Mobile Phones* [13] a method for estimating crowd density by using a mobile phone to scan the environment for discoverable bluetooth devices is presented. That this method works has the reason, that many people have their bluetooth devices already in discoverable mode [13]. The authors improved the simple approach to count how many bluetooth devices are in a special area at the same time and estimate the crowd density. The paper has shown that just few data from bluetooth scans is enough to determine the crowd density [13]. This information could be a new approach for

crowd monitoring. If the crowd density is known other already working monitoring techniques could be exploited to inform the user about risks and other important information.

5. PRIVACY ISSUES

There has been much discussion recently concerning the need for privacy in ubiquitous computing, and particularly in the case of surveillance [10]. Humans feel uncomfortable when they know that they are monitored. This aspect is discussed detailed in the paper *Being watched or being special: how I learned to stop worrying and love being monitored, surveilled, and assessed* [16]. Nevertheless there is nowadays a great interest in vision monitoring in all kind of situations and environments. The main goals would be security, resource management or advertising [9]. The advantages of for example security and the apparent disadvantage namely the loss of privacy are in conflict with each other.

In case of crowd monitoring there are two solutions for this problem. The first is sensitizing the crowd for crowd monitoring and put the privacy aspect in the rear. The second solution is monitor the crowds without people tracking or models. Sensitizing people to give away personal information has taken place over the last years in a big style. One of the best examples is Google-Now. The application notifies personal preferences and gives suggestions to the user. It even examines the personal e-mails for information that can be useful. Since android version 4.1 every smart-phone contains Google-Now and it's accepted. March 2013 Google announced that nearly one billion android smart-phones are activated. 59 percent of them use android version 4.1 or higher. Even if only half of the users use Google-Now, there are around 350 million people, which allow the invasion of privacy.¹ Inferring thereof a good way to sensitize people for monitoring is showing them the advantages.

The more vivid solution is to monitor the crowd without offending the individual privacy. Do not pay attention on individual privacy becomes an especially acute problem for crowd monitoring with computer vision for two reasons. First the perception of compromised privacy is particularly strong for technology which, by default, keeps a visual record of people's actions. Second the current approaches to vision-based monitoring are usually based on object tracking or image primitives, such as object silhouettes or blobs, which imply some attempt to "identify" or "single out" the individual [9]. I will illustrate a method with the following example orientating towards the paper *Privacy Preserving Crowd Monitoring: Counting People without People Models or Tracking* [9]. To get this introduced a new formulation for surveillance technology, which is averse to individual tracking and, consequently, privacy preserving is needed. The used crowd monitoring model is counting how many people walk through a certain area, with taking care of the direction and estimate the crowd density. Successful crowd counting depends on effective crowd segmentation. The crowds are splitted in two groups. The ones who move towards the camera and the ones who move away. Special algorithms are used to find out the direction of the moving people. As mentioned in the section *video monitoring* errors occur if people can't be identified as moving objects or if they move to fast, for example on bicycles. The difference to non private methods is, that

¹<http://www.google.com/intl/de/landing/now>

the objects are no longer seen as humans, but as moving objects. That confer benefits in privacy and also in accuracy, cause here are not only humans detected, also other moving objects like dogs for example, which also contribute to crowd density.

6. OPPORTUNITIES

The opportunities crowd monitoring provides are mainly in the region safety. Preventing chaos and in case of an emergency injured visitors at an event or in public has highest priority level. Nowadays human factors play still a role in crowd monitoring. One goal should be to automate all parts, like the monitoring by itself, in case of safety risks the redirection of the crowd and sending for example emergency doctors directly to an accident. The main point in future is that huge assemblages of people harbor no risk factors for the participants.

7. CONCLUSION

This paper gives an overview about crowd monitoring and the inevitably challenges. The goal of crowd monitoring is to afford safety, while not intervening in the users individual privacy. The paper has shown that it is possible to use well-established techniques for monitoring and collecting data on crowd behaviour. Although there are still many problems to deal with, crowd monitoring plays a big role in safety management in future.

8. REFERENCES

- [1] A. G. Abuarafah, M. O. Khozium, and E. AbdRabou, "Real-time crowd monitoring using infrared thermal video sequences," *Journal of American Science*, vol. 8, no. 3, pp. 133–140, 2012.
- [2] I. Carreras, D. Miorandi, A. Tamlin, E. R. Ssebaggala, and N. Conci, "Crowd-sensing: Why context matters," in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2013 IEEE International Conference on*, pp. 368–371, IEEE, 2013.
- [3] A. C. Davies, J. H. Yin, and S. A. Velastin, "Crowd monitoring using image processing," *Electronics & Communication Engineering Journal*, vol. 7, no. 1, pp. 37–47, 1995.
- [4] M. Wirz, D. Roggen, and G. Troster, "User acceptance study of a mobile system for assistance during emergency situations at large-scale events," in *Human-Centric Computing (HumanCom), 2010 3rd International Conference on*, pp. 1–6, IEEE, 2010.
- [5] D. Boyd and K. Crawford, "Six provocations for big data," 2011.
- [6] J. Manyika, M. Chui, B. Brown, J. Bughin, R. Dobbs, C. Roxburgh, and A. H. Byers, "Big data: The next frontier for innovation, competition, and productivity," 2011.
- [7] M. Kantardzic, *Data mining: concepts, models, methods, and algorithms*. John Wiley & Sons, 2011.
- [8] A. Blum, A. Kalai, and J. Langford, "Beating the hold-out: Bounds for k-fold and progressive cross-validation," in *Proceedings of the Twelfth Annual Conference on Computational Learning Theory*, COLT '99, (New York, NY, USA), pp. 203–208, ACM, 1999.

- [9] A. B. Chan, Z.-S. Liang, and N. Vasconcelos, “Privacy preserving crowd monitoring: Counting people without people models or tracking,” in *Computer Vision and Pattern Recognition, 2008. CVPR 2008. IEEE Conference on*, pp. 1–7, IEEE, 2008.
- [10] M. Wirz, T. Franke, D. Roggen, E. Mitleton-Kelly, P. Lukowicz, and G. Troster, “Inferring crowd conditions from pedestrians’ location traces for real-time crowd monitoring during city-scale mass gatherings,” in *Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2012 IEEE 21st International Workshop on*, pp. 367–372, IEEE, 2012.
- [11] M. Wirz, T. Franke, D. Roggen, E. Mitleton-Kelly, P. Lukowicz, and G. Troster, “Inferring crowd conditions from pedestrians’ location traces for real-time crowd monitoring during city-scale mass gatherings,” in *Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2012 IEEE 21st International Workshop on*, pp. 367–372, IEEE, 2012.
- [12] B. C. Welsh and D. Farrington, “Is cctv effective in preventing crime in public places?,” *Evidence Based Policing*, pp. 265–268, 2011.
- [13] J. Weppner and P. Lukowicz, “Collaborative crowd density estimation with mobile phones,” *Proc. of ACM PhoneSense*, 2011.
- [14] D. Yang, G. Xue, X. Fang, and J. Tang, “Crowdsourcing to smartphones: incentive mechanism design for mobile phone sensing,” in *Proceedings of the 18th annual international conference on Mobile computing and networking*, pp. 173–184, ACM, 2012.
- [15] T. NAGALAKSHMI, “A study on usage of cctv surveillance system with special reference to business outlets in hyderabad,” 2012.
- [16] E. Robles, A. Sukumaran, K. Rickertsen, and C. Nass, “Being watched or being special: how i learned to stop worrying and love being monitored, surveilled, and assessed,” in *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pp. 831–839, ACM, 2006.

Security Challenges for the Internet of Things

Florian Kovacs
Universität Passau
Fakultät für Informatik und Mathematik
Innstr. 33
94032 Passau, Germany
kovacs@fim.uni-passau.de

Kurzfassung

In der heutigen Zeit hält das Internet in immer mehr Bereichen Einzug, so auch in Geräten, die man auf den ersten Blick nicht mit der digitalen Welt in Verbindung bringen würde, beispielsweise in Haushaltsgeräten. Dadurch werden auch immer mehr Daten erfasst, die viel über das Verhalten und die Lebensweise des Benutzers aussagen können. Aufgrund der Verbindung zum Internet werden diese Daten dann auch zu einem Teil des World Wide Webs, was prinzipiell externen Zugriff darauf möglich macht. Dies hat zur Folge, dass diese sensiblen Daten, die Einsicht in die Privatsphäre des Benutzers erlauben, in besonderem Maße geschützt werden müssen. Dieses Paper gibt nun einen Einblick in mögliche Lösungen dieses Problems und erklärt die Wichtigkeit der schnellstmöglichen Einführung von Sicherheitsstandards im Internet der Dinge.

Keywords

Encryption, Internet of Things, Wireless Sensor Networks

1. EINLEITUNG

Der Begriff "Internet der Dinge" bezeichnet den aktuellen Trend, dass immer mehr Geräte mit dem Internet verknüpft werden [1]. Diese Geräte zeichnen sich dadurch aus, dass sie autonom mit dem Internet interagieren und somit eigens, beispielsweise mittels RFID-Chips, identifiziert werden müssen [13]. Man kann dabei jedes physische Objekt mit so einem Computerchip ausstatten, der eine eindeutige Identifizierung gewährleistet. Dieser Chip kann auch in eine größere Struktur eingebunden werden, die beispielsweise Sensoren und Datenspeicher enthält, und diese dann auslesen oder beschreiben. Damit ergeben sich neue Möglichkeiten, die reale Welt mit der virtuellen zu verbinden. Beispiele dafür sind Autos mit Internetzugriff, die Staus oder Fahrzustände erkennen, Sensoren für wissenschaftliche Messungen, in etwa Wetterstationen und Luftmessgeräte, oder Kühlschränke, die ihren Inhalt erfassen können,. Die dabei

erfassten Daten können hochsensibel in Bezug auf die Privatsphäre von Personen sein. Um sie erfolgreich vor unbefugtem Zugriff zu schützen, werden daher Sicherheitsmaßnahmen angewendet. Diese können in etwa die Authentizität der an der Kommunikation beteiligten Geräte oder eine verschlüsselte Datenübertragung sicherstellen. Ein Beispiel für eine sicherheitsrelevante Anwendung des Internets der Dinge ist das SmartPiggy, welches Informationen über angespartes Geld über das Internet zugänglich macht [11]. Weil dabei kaum Sicherheitsmechanismen eingebaut wurden, existiert ein erhöhtes Risiko, dass auf die dabei gesammelten privaten Daten unauthorisierter Zugriff erfolgen kann. Da diese Daten finanzieller Natur sind, wäre deren Codierung eindeutig notwendig.

2. ALLGEMEINE PROBLEMATIK

Da das Thema Sicherheit im Internet einen großen Stellenwert einnimmt, findet es auch im Internet der Dinge Beachtung. Dabei treten zum Teil schon bekannte Probleme auf, aber mit der typisch minimalistischen Leistung von Sensoren etc. rücken auch neue Aufgaben in den Fokus, die es zu lösen gilt.

2.1 Probleme

Big Data ist auf dem Vormarsch [9]. Immer mehr Daten aus immer mehr Bereichen des täglichen Lebens werden gesammelt, auch sensible Daten aus der Privatsphäre der Menschen. Dass man mit diesen Daten Umsatz generieren kann, haben inzwischen viele Unternehmen erkannt und reagieren darauf mit immer mehr Datensammlung und -analyse. Jedoch können auch höchstpersönliche Informationen, sofern sie nicht gesichert übertragen werden, abgehört und missbraucht werden. Geräte zur Erhebung sensibler Daten müssen daher Verschlüsselungsmechanismen aufweisen, welche die Kommunikation chiffrieren.

Auch allgemeine Sensor-Netzwerke haben einen Sicherheitsanspruch. Wenn man die Datensicherheit im Internet der Dinge betrachtet, kann man grob zwei Phasen unterscheiden: Die Phase, in der Daten von eingebetteten Datenspeichern gelesen werden bzw. darauf geschrieben werden und die Phase der Datenübertragung im Internet selbst. In letzterer orientieren sich die Sicherheitsanforderungen an den bisher bestehenden Ansprüchen, die für den Datentransfer im Internet gelten. Deshalb wird im Folgenden nur die Sicherheit in der ersten Phase behandelt.

Ein großes Problem stellt die beschränkte Rechenleistung von eingebetteten Systemen dar, die nur eingeschränkt für komplexe Verschlüsselungen tauglich ist. So ist es etwa äu-

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Advances in Embedded Interactive Systems '14 Passau, Germany
Volume 2, Issue 3 (October 2014). ISSN: 2198-9494

berst aufwendig und unpraktikabel, Daten permanent über verschlüsselte Kanäle zu übertragen oder zu empfangen. Dieses Problem wird durch die typischerweise große Anzahl von Geräten in Netzwerken noch verstärkt, da dabei viele Transaktionen nötig sind, die alle mögliche Angriffspunkte sind [3]. In Korrelation dazu steht die zur Verfügung stehende Energie, welche bei kleinen Systemen konzeptbedingt gering ausfällt. Ergo sind Lösungen zu bevorzugen, die zwar energiearm und mit geringer Rechenleistung operieren können, zugleich aber auch die Datensicherheit signifikant verbessern.

Eine zentrale Herausforderung bei der Entwicklung von Transfermethoden für Daten ist die Authentifizierung. Damit ist die Identifizierung eines Gerätes beim Auslesen oder Schreiben von Daten gemeint, wodurch unauthorisiertem Zugriff vorgebeugt wird [12]. Das ist dem Umstand zu verdanken, dass dann nur Geräte, die eine Berechtigung dafür besitzen, Lese- und Schreibrechte auf gespeicherte Daten erhalten.

Des Weiteren gibt es wenige Standards, die man bei der Software eingebetteter Systeme als uneingeschränkt kompatibel und einsetzbar voraussetzen kann. Für verschiedene Systeme müsste man demnach verschiedene Lösungen entwickeln. Außerdem sind bisher bestehende Regelungen aufgrund der verschiedenen Gesetzeslagen unterschiedlicher Staaten alles andere als einheitlich. Daher sind die sicherheitsspezifischen Anforderungen von Land zu Land anders, es werden also unterschiedliche Umsetzungen für unterschiedliche Land benötigt [13].

Zudem gilt wie im Computer-Sektor das Mooresche Gesetz, welches eine grobe Schätzung der Leistungssteigerung von Computerchips ermöglicht¹. Jedoch ist dieser Leistungszuwachs auch bei attackierenden Systemen vorhanden, man kann also nicht allein auf eine zukünftig höhere Leistungsfähigkeit setzen.

2.2 Lösungen

Um die mangelnde Rechenleistung zu kompensieren ist es möglich, spezielle effiziente Algorithmen verwenden, um den Rechenaufwand niedrig zu halten. Auch der Energieverbrauch lässt sich begrenzen, indem man Verfahren anwendet, die mit möglichst wenig Aufwand möglichst sichere Verschlüsselungen umsetzen. Um die Authentifizierung von Geräten zu realisieren, werden zumeist Handshake-Protokolle verwendet, in denen die Verschlüsselung von Zufallswerten auf Übereinstimmung abgeprüft werden. Im Bereich der eingebetteten Systeme wird versucht, so einen Handshake ressourcenschonend zu implementieren. Beispielsweise kann das so aussehen, dass sich nur das lesende/schreibende Gerät bei dem Gerät, auf das zugegriffen wird (in etwa ein RFID-Tag), authentifiziert. Ein Weg zur Vermeidung unnötiger Verschlüsselung (und auch Datenübertragung) ist die Aggregation von gesammelten Daten, bei welcher Informationen direkt im eingebetteten System verarbeitet und zusammengefasst werden und die Zusammenfassung dann übertragen wird [2, 6].

Da die heutigen Sicherheitsanforderungen länderspezifisch sind, gibt es noch keine universelle Lösungen, dennoch ist die Schaffung internationaler Rahmenbedingungen vonnöten [13]. Sofern solche globalen Regelungen nicht von den

¹Dieses Maß wird laut dem Artikel "Keeping Up with Moore's Law" des Dartmouth Undergraduate Journal of Science weiterhin Bestand haben

Unternehmen forciert werden, kommt man nicht umhin eine andere internationale Vereinigung zu erstellen oder damit zu beauftragen. Dies würde nicht nur die Portabilität und Kompatibilität der Systeme untereinander erhöhen, sondern auch den Entwicklungsaufwand positiv beeinflussen. So gibt es bereits Überlegungen, Geräte in das TCP/IP-System einzugliedern, bei dem die Infrastruktur schon vorhanden ist und damit nur minimaler Aufwand zur Anpassung betrieben werden muss [7].

3. UMSETZUNG

Da die Rechenleistung von eingebetteten Systemen typischerweise nicht so hoch ist wie die von Computern oder Smartphones, werden Verschlüsselungsalgorithmen benötigt, die effizient und gleichzeitig ressourcenschonend sind. Diese Algorithmen müssen dabei sowohl beim eingebetteten System als auch beim Auslese-/Schreibgerät durchführbar sein. Dabei ist beim eingebetteten System meist ein RFID-Tag für die Datenübertragung eingebaut, welches durch ein Lesegerät, das ein elektromagnetisches Feld erzeugt, aktiviert wird und dann zum Datentransfer verfügbar ist.

3.1 Authentifizierung

Um die Berechtigung eines Gerätes festzustellen, wird zu meist ein vertilter Schlüssel verwendet, den die beteiligten Geräte besitzen müssen. Ein Gerät A kann sich nun bei einem anderen Gerät B authentifizieren, indem es eine empfangene Zufallszahl von B mit dem gemeinsamen Schlüssel K kodiert und zurückschickt. Da Gerät B die Zufallszahl auch verschlüsseln kann, kann es überprüfen, ob A dafür den selben Schlüssel verwendet hat. In diesem Fall weiß Gerät B, dass A den selben Schlüssel besitzt und somit authentifiziert ist [5]. Dieses Handshake-Protokoll ist im Folgenden visualisiert, wobei K(z) die Verschlüsselung von z mit der Chiffre K bezeichnet:

```
B → A : Zufallszahl z
B ← A : K(z)
B → A : Bestätigung/Daten
```

3.2 Keying-Verfahren

Wenn in einem Netzwerk Schlüssel zur Authentifizierung eingesetzt werden, muss auch sichergestellt werden, dass diese Schlüssel komplex genug sind um nicht geknackt zu werden und dass sie nur berechtigten Geräten zur Verfügung gestellt werden. Ansonsten können Angreifer einfach Schlüssel abgreifen und somit Zugang zum Netzwerk erhalten. Die einfachste Form einer Schlüsselverbreitung, nämlich das Vorhandensein eines universellen Schlüssels innerhalb des Systems, kommt aus Sicherheitsgründen kaum in Frage. Auch eine gegenteilige Umsetzung, die einem Paar von Geräten, das miteinander kommunizieren will, einen eigenen Schlüssel zuweist, ist zu komplex umzusetzen und würde nur unnötigen Ressourcenverbrauch verursachen. Somit wird meist eine Gruppe von Geräten mit dem gleichen Schlüssel ausgestattet, was eine Lösung mit den Vorteilen beider Extreme darstellt. Eine weitere Methode, Keying umzusetzen, ist die Errichtung eines Schlüsselpools [4]. Dabei werden die Authentifizierungsschlüssel per Index referenziert, es dringen also keine Informationen über die Schlüssel selbst nach außen, sondern nur die Nummer des Schlüssels. Bei der Kommunikation zweier Geräte werden nun die Schlüssel beider Geräte per XOR verknüpft, man erhält dann einen einzi-

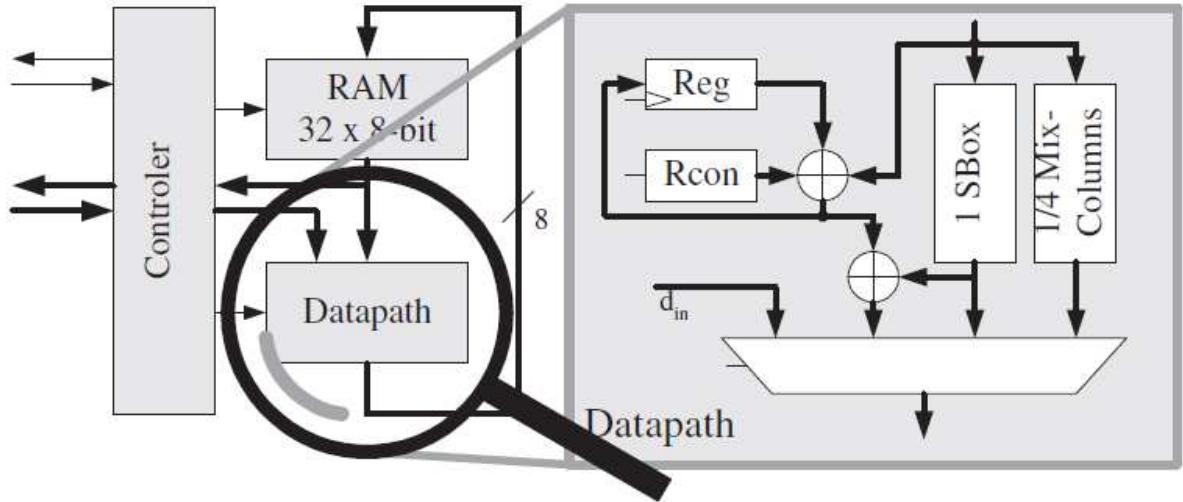


Figure 1: Architektur eines AES-Verschlüsselungsmoduls

gen Schlüssel, der fortan Übertragungen zwischen den Geräten verschlüsselt. Dies bedeutet einen zusätzlichen Sicherheitsgewinn, da die Verschlüsselung nun von zwei Geräten abhängt, die beide vom Angreifer korrumptiert werden müssen, um an Daten zu gelangen.

3.3 AES-Algorithmus

Der Advanced Encryption Standard (AES) [5] ist ein symmetrischer Verschlüsselungsalgorithmus, der 2001 vom US-amerikanischen National Institute of Standards and Technology als Kryptographiestandard festgelegt wurde. Er operiert auf quadratischen Blöcken von Daten und manipuliert diese mit verschiedenen Verfahren. Die Manipulationen können dabei linear, nichtlinear oder abhängig von dem gegebenen Schlüssel sein. Dabei sind folgende Operationen möglich:

1. SubBytes ersetzt jedes Element eines Blocks, wobei meist look-up-Tabellen verwendet werden
2. ShiftRows verschiebt jede Zeile um einen Offset, welcher der Zeilennummer entspricht, siehe 2
3. MixColumns multipliziert jede Tabellenspalte mit einer Konstante
4. Bei AddRoundKey wird der Schlüssel mit dem aktuellen Block per XOR-Verknüpfung verändert

Ein Modul, welches diesen Algorithmus umsetzt, kann sehr einfach aufgebaut sein, wie die Grafik 1 zeigt. Es wird lediglich ein Controller, einen Arbeitsspeicher und ein sogenannter Datenpfad, welcher den eigentlichen Verschlüsselungsvorgang durchführt, benötigt. AES ist daher eine gelungene Umsetzung eines Verschlüsselungsalgorithmus im Lightweight Design und gut einsetzbar in eingebetteten Systemen wie sie im Internet der Dinge vorhanden sind.

3.4 TinySec

Die exemplarische Implementierung TinySec [8] ist ebenfalls als eine solche leichtgewichtige Sicherheitsarchitektur,

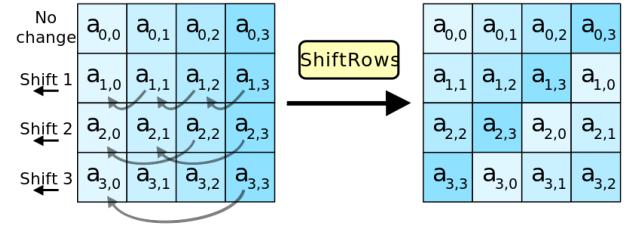


Figure 2: Verschiebungsoperation auf Zeilen des Datenblocks

welche extra mit Fokus auf dem Internet der Dinge entwickelt wurde. Wie AES operiert dieses Verfahren auf Datenblöcken, wobei zur Erhöhung der Sicherheit auch noch Initialisierungsvektoren² eingesetzt werden. Dadurch wird die Verschlüsselung dynamisiert, was dazu führt, dass die Verschlüsselung eines Textblocks von dessen Position innerhalb des Textes abhängt. Zur Codierung der Datenblöcke standen verschiedene Algorithmen zur Auswahl, darunter auch AES, Triple-DES und RC5, aber letztlich entschieden sich die Macher dieses Verfahrens für den Skipjack-Algorithmus, der besonders effizient arbeitet. Bei der Kommunikation innerhalb des Netzwerks wird vor allem auf die Authentifizierung von Geräten und Nachrichten geachtet, die Verschlüsselung gesendeter Daten wird optional nur bei sensiblen Daten angewendet. Dadurch wird nicht unnötig Energie und Rechenleistung verbraucht.

²Initialisierungsvektoren sind Blöcke von Zufallszahlen, die dazu dienen, Muster (Wiederholungen) in einem verschlüsselten Text zu vermeiden. Gleiche Textblöcke werden also unterschiedlich verschlüsselt. Meist ist die Verschlüsselung von bereits verarbeiteten Datenblöcken abhängig. Definition von http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Initialization_vector.html

3.5 Andere Verfahren

Als weitere Verschlüsselungsverfahren wären Rivest shamus adelman (RSA-Algorithmus) und Elliptic curve cryptography (ECC) zu nennen, welche im Gegensatz zu AES und TinySec asymmetrisch sind [12]. Das heißt, dass miteinander kommunizierende Geräte keinen gemeinsamen Schlüssel benötigen, um sich zu authentifizieren. Diese Anwendungen werden hauptsächlich für digitale Signaturen und zur Schlüsseldistribution verwendet. Als Vorgänger von AES kann man DES (Data Encryption Standard) bezeichnen, welcher allerdings wegen nur 56 Bit Schlüssellänge als nicht mehr sicher gilt. Durch eine Schlüsselerweiterung wird der Algorithmus selbst, der dahinter steht, auch heute noch verwendet und als Triple-DES bezeichnet[10].

4. DISKUSSION

Bei einer so weitreichenden und wichtigen Entwicklung wie der des Internets der Dinge sind Regelungen über den Umgang mit dieser Technologie unvermeidbar. Vor allem Privatsphäre und Datensicherheit sind in diesem Feld zu betrachten. Um diese Aspekte umsetzen zu können, werden weltweite Standards erforderlich, die dieses System transparenter und übersichtlicher gestalten. Also nicht nur Standards bei der Hardware, sondern auch bei Verschlüsselungsverfahren und Protokollen, welche hauptsächlich Datensicherheit gewährleisten. Möchte man beispielsweise Geräte unterschiedlicher Hersteller in ein System integrieren, so ist es von großem Vorteil, wenn sie von vorne herein zueinander kompatibel sind und nicht erst neu konfiguriert oder programmiert werden müssen. Dies ist vor Allem für die Wirtschaft von Bedeutung, da solche Anpassungen immer mit Kosten verbunden sind.

Die Frage, die noch im Raum steht, ist die nach der Zuständigkeit für die Normierung. Rudolf H. Weber unterscheidet dabei zwei wahrscheinliche Szenarien [13]: Einerseits die Festlegung der Standards von staatlicher Seite, andererseits die Selbstregulierung innerhalb der Wirtschaft. Bei staatlicher Regulierung tritt jedoch das Problem auf, dass die Staaten der internationalen Gemeinschaft nicht in allen Themen übereinstimmen werden und somit eine einheitliche Lösung schwer zu erzielen ist. Wirtschaftliche Selbstregulierung hingegen hat den Nachteil, dass sich solche Regelungen meist nur innerhalb eines bestimmten Rahmens (innerhalb eines Landes oder einer Ländergemeinschaft) bewegen, was wiederum das Problem der Heterogenität zur Folge hat. Weber schlägt daher eine Hybridlösung dar, die die Vorteile beider Konzepte vereinen soll, und nur wirklich wichtige Aspekte unter staatliche Kontrolle stellt.

5. ABSCHLUSS

Wie schon im World Wide Web, ist auch im Internet der Dinge das Thema Sicherheit und Privatsphäre von entscheidender Bedeutung. Ob man diese Problematik nun durch neue algorithmische Lösungen angeht oder durch die Festlegung von Standardprotokollen, das Ziel ist das gleiche, nämlich die gefahrlose Integration von intelligenten Geräten in das weltweite Netzwerk. Es wird bereits von verschiedenen Seiten daran gearbeitet, sowohl staatliche Stellen als auch Konzerne und private Vereinigungen sind sehr daran interessiert, die bestehenden Sicherheitslücken zu schließen. Dabei ist nicht nur maximale Sicherheit entscheidend, sondern auch eine praktikable Umsetzung mit geringem Energiever-

brauch und Rechenaufwand. Die Devise lautet also, maximale Sicherheit mit minimalem Aufwand sicherzustellen.

6. REFERENCES

- [1] L. Atzori, A. Iera, and G. Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.
- [2] C. Castelluccia, E. Mykletun, and G. Tsudik. Efficient aggregation of encrypted data in wireless sensor networks. In *Mobile and Ubiquitous Systems: Networking and Services, 2005. MobiQuitous 2005. The Second Annual International Conference on*, pages 109–117. IEEE, 2005.
- [3] H. Chan and A. Perrig. Security and privacy in sensor networks. *Computer*, 36(10):103–105, 2003.
- [4] R. Di Pietro, L. V. Mancini, and A. Mei. Random key-assignment for secure wireless sensor networks. In *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pages 62–71. ACM, 2003.
- [5] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong authentication for RFID systems using the AES algorithm. In *Cryptographic Hardware and Embedded Systems-CHES 2004*, pages 357–370. Springer, 2004.
- [6] W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher. Pda: Privacy-preserving data aggregation in wireless sensor networks. In *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, pages 2045–2053. IEEE, 2007.
- [7] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle. Security Challenges in the IP-based Internet of Things. *Wireless Personal Communications*, 61(3):527–542, 2011.
- [8] C. Karlof, N. Sastry, and D. Wagner. TinySec: a link layer security architecture for wireless sensor networks. In *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pages 162–175. ACM, 2004.
- [9] V. Mayer-Schönberger and K. Cukier. Big Data, 2013.
- [10] F.-X. Standaert, G. Rouvroy, and J.-J. Quisquater. FPGA implementations of the DES and triple-DES masked against power analysis attacks. In *Field Programmable Logic and Applications, 2006. FPL'06. International Conference on*, pages 1–4. IEEE, 2006.
- [11] T. Stockinger, M. Koelle, P. Lindemann, L. Witzani, and M. Kranz. SmartPiggy: A Piggy Bank that talks to your Smartphone. In *Proceedings of the 12th International Conference on Mobile and Ubiquitous Multimedia*, page 42. ACM, 2013.
- [12] H. Suo, J. Wan, C. Zou, and J. Liu. Security in the internet of things: a review. In *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, volume 3, pages 648–651. IEEE, 2012.
- [13] R. H. Weber. Internet of Things—New security and privacy challenges. *Computer Law & Security Review*, 26(1):23–30, 2010.

Mit Gamification zum Eco-Driving: die Zukunft vor den Augen oder doch im Ohr?

Magdalena Murr

Universität Passau

Innstr. 43

94032 Passau, Germany

murr04@stud.uni-passau.de

ABSTRACT

Der durchschnittliche Erwachsene verbringt heutzutage sehr viel Zeit im Auto und so ist es nicht verwunderlich, dass die Ausstattung desselben in den letzten Jahrzehnten stetig komfortabler und komplexer geworden ist. Von der Klimaanlage über Radio, CD-Player, Navigationssystem und Freisprecheanlage bieten Autos heute ein hohes Maß an Komfort und Unterhaltung [1]. Dieses Paper befasst sich mit dem Aspekt *Gamification* im Automobilbereich.

Zu diesem Zweck wird zunächst allgemein der Begriff *Gamification* erklärt. Anschließend werden Anwendungen für *Eco-Driving* vorgestellt.

Im zweiten Teil der Arbeit gehe ich konkret auf eines der Hauptprobleme bei solchen Systemen ein: die Ablenkung des Fahrers. Es folgt eine Diskussion über die möglichen Arten des Feedbacks bei solchen Anwendungen und ihre Eignung bezüglich angestrebter *Gamification* und minimaler Ablenkung des Fahrers.

Keywords

Gamification, Eco-Driving, Ablenkung, Feedback

1. EINLEITUNG

Mit den häufig wiederkehrenden Prognosen zum Ende der Ölreserven auf der Erde binnen 40 Jahren¹, den ständig steigenden Spritpreisen und der zunehmenden Umweltbelastung vor allem durch CO₂-Emissionen² liegt es im Allgemeinen Interesse (vor allem mit Blick auf zukünftige Generationen) Benzin einzusparen. Es gibt jedoch bisher kein Gesetz, das einen ökologischen und ökonomischen Fahrstil fordert, weil es wohl schwierig umzusetzen wäre.

¹http://www.focus.de/wissen/klima/tid-14230/energie-mythen-mythos-das-oel-reicht-noch-40-jahre_aid_398164.html

²<http://epp.eurostat.ec.europa.eu/portal/page/portal/environment/data/database>

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Advances in Embedded Interactive Systems '14 Passau, Germany
Volume 2, Issue 3 (October 2014). ISSN: 2198-9494

Eine andere Tatsache, die zunächst aus dem Zusammenhang gerissen scheint: Menschen spielen gerne Spiele. Dieses Verhalten trat schon vor mehreren tausend Jahren auf [5] und in der Neuzeit hat sich daran nichts geändert: Onlinespiele beispielsweise (selbst kostenpflichtige) erfreuen sich allgemeiner Beliebtheit, nicht nur unter Kindern und Jugendlichen.

Knüpfen wir eine Verbindung zwischen diesen beiden Erkenntnissen, so führt uns das zu *Gamification*: Wir wollen die Menschen motivieren, Sprit zu sparen. Die Menschen spielen gerne Spiele. Folglich designen wir Anwendungen, die spielerisch zu einem ökologischen und ökonomischen Fahrstil anregen. Mit der richtigen Umsetzung wird umweltbewusstes Verhalten belohnt und gegenteiliges Verhalten bestraft.

Tatsächlich sind auch schon einige solcher Systeme im Einsatz, wie z.B. Fiats "eco:Drive"³, bei dem man mit umweltbewusstem Fahren Punkte, sogenannte "eco:Badges", sammeln und damit zusammen mit anderen Spielern eine virtuelle "grüne" Stadt "eco:Ville" aufbauen kann. Ein anderes Beispiel wäre Fords "FordGauge"⁴, ein Programm, das neben der Geschwindigkeitsanzeige (auf dem Driver-Centered Combi-Display des Autos) grüne Blätter wachsen, bzw. verwelken lässt, je nach Effizienz des Fahrstils. In Abschnitt 2 wird das Design-Konzept *Gamification* vorgestellt und es werden in Abschnitt 2.1 Anwendungen, bei denen dieses Konzept zum Einsatz kommt vorgestellt. In Abschnitt 2.2 wird das Problem der Ablenkung des Fahrers durch solche Applikationen herausgearbeitet und in Abschnitt 2.3 werden verschiedene Arten des Feedbacks und ihre Tauglichkeit im Bezug auf *Gamification* und möglichst geringe Ablenkung des Fahrers diskutiert.

2. GAMIFICATION IM AUTO

Deterding et al. [3] definieren *Gamification* als die Verwendung von Elementen aus der Spiele-Modellierung in einem anderen Kontext, der zunächst einmal nichts mit Spielen zu tun hat. Anders gesagt baut man in eher reizlosen Szenarien Spiele ein, um Benutzer zu motivieren eine bestimmte Handlung durchzuführen. Bei der Gestaltung eines Spiels muss man einige Aspekte beachten. Laut McGonigal [9] muss jedes Spiel folgende Merkmale aufweisen:

1. Ziel: das Ergebnis, auf das der Spieler hinarbeitet
2. Regeln: ein Handlungsrahmen, der die Möglichkeiten zum Erreichen des Ziels einschränkt

³<http://www.fiat.com/com/PublishingImages/ecodrive-site/de/default.htm>

⁴<http://www.ford.com/cars/cmax/features/Feature4/#page=Feature4>

3. Feedback System: mithilfe von Punkten, Levels, o.Ä. wird dem Spieler gezeigt, wie nah er seinem Ziel bereits ist
4. freiwillige Teilnahme: Garantie, dass alle Spieler das Ziel und die Regeln akzeptieren und sich sicher fühlen, weil sie jederzeit aussteigen können

Eine große Rolle bei allen Tätigkeiten spielt auch der Ursprung der Motivation. Man unterscheidet zwischen intrinsischer und extrinsischer Motivation. Ryan und Deci [11] erklären diese folgendermaßen: Ein intrinsisch motivierter Mensch erlangt Befriedigung aus der Handlung selbst, während extrinsisch motivierte auf eine Belohnung hoffen oder eine Strafe vermeiden wollen indem sie die Handlung ausführen (hier ist die eigentliche Handlung nebensächlich, es geht um die Wirkung/Folgen). Es liegt in der Natur eines Spiels, dass es bei den meisten Menschen intrinsische Motivation hervorruft, jedoch müssen auch jene angesprochen werden, bei denen das nicht der Fall ist. Es gilt folglich bei der Modellierung von Spielen darauf zu achten, dass eine Balance gefunden zwischen diesen beiden Motivationsquellen gefunden wird.

Das Konzept Gamification wird laut Diewald et al. [5] im Automobilbereich bereits vielfältig eingesetzt, z.B. als Motivation für sicheres Fahren, zur Navigation, oder auch um Fahrer spielerisch mit der Menüstruktur vertraut zu machen. Ein großes Feld macht das sogenannte Eco-Driving aus, zu dem wir im Folgenden einige Beispiele genauer beleuchten werden.

2.1 Eco-Driving

Mit "Eco-Driving" wird in diesem Paper die Anpassung des Fahrstils durch den Autofahrer bezeichnet, sodass ein möglichst geringer Kraftstoffverbrauch erreicht wird. Die Idee, Fahrzeugführer mit einem Programm darin zu unterstützen sparsam zu fahren ist nicht neu (schon 1989 gab es derartige Ansätze [12]), rückt jedoch in den letzten Jahren immer mehr in das Interesse der Forscher. Laut Studien kann der Autofahrer den Benzinverbrauch durch Anpassung seines Fahrverhaltens um bis zu 25% senken [8]. Im Jahr 2012 wurden 266.258,6 Tausend Tonnen Kraftstoff (Benzin, Dieselöl und Gasöl ohne Biokomponenten) in der Europäischen Union (28 Länder) verbraucht⁵. Eine Einsparung von 25% entspräche hier 66.564,65 Tausend Tonnen Öl pro Jahr allein in der Europäischen Union. Im Folgenden werden Anwendungen vorgestellt, die mit *Gamification* den Fahrer motivieren, spritsparend zu fahren. Dabei unterstützen sie ihn, indem sie Tipps geben, wie er dieses Vorhaben am besten umsetzen kann.

2.1.1 EcoChallenge

Ecker et al. [6] haben den Prototyp *EcoChallenge* entwickelt. *EcoChallenge* gibt dem Fahrer Feedback in Form einer Anzeige von

1. Effizienz von aktuellem Beschleunigungs- oder Bremsvorgang
2. Einem Ranking im Vergleich mit anderen Nutzern der Anwendung
3. einer Historie, die den eigenen Geschwindigkeitsverlauf und den besten Verlauf auf dieser Strecke anzeigt, ebenso wie die erlangten Bonuspunkte auf dieser Fahrt

Zur Visualisierung stehen drei verschiedene Displays zur Verfügung: ein frei programmierbares Instrument-Cluster,

⁵<http://epp.eurostat.ec.europa.eu/portal/page/portal/energy/data/database>

ein Head-Up-Display und ein Central-Information-Display im Zentrum des Fahrzeugs.

EcoChallenge macht guten Fahrstil abhängig von schneller Beschleunigung gepaart mit möglichst langem gleichmäßig schnellem Fahren und wenig abrupten Bremsmanövern. In einer Studie mit einem Testfahrzeug und 37 Testteilnehmern war die Akzeptanz sehr hoch, das heißt die Benutzer fühlten sich durch die Anwendung nicht negativ beeinträchtigt. Im Gegenteil gaben die Teilnehmer an, dass sie sich motiviert gefühlt hätten und Spaß am Fahren hatten.

2.1.2 GAFU

Magaña und Organero entwickelten das Spiel GAFU [8]. GAFU gibt dem Spieler in Echtzeit Audio-Feedback über das Smartphone in Form von Warnungen (sobald ineffizientes Fahren diagnostiziert wird). Außerdem erhält man am Ende der Fahrt eine visuelle Übersicht über erreichte Punkte, Spritverbrauch, etc. Diese Daten kann man mit Freunden über ein soziales Netzwerk teilen und vergleichen.

Ein effizienter Fahrstil wird an folgenden Kriterien festgemacht: keine zu hohe Geschwindigkeit, kein ruckartiges Beschleunigen/ Bremsen, kein unnötiges Beschleunigen/ Bremsen, stetige Geschwindigkeit, geringe Motordrehzahl. Die zur Beurteilung dieser Kriterien benötigten Daten erhält die Anwendung direkt vom Fahrzeug. Die Warnungen/Tipps werden nach folgendem Muster generiert: Anteil an schnell gefahrener Strecke, Anteil an mit hoher Motordrehzahl gefahrener Strecke, Anteil an plötzlichen Beschleunigungs-/ Bremsmanövern und Anteil an nicht mit stetiger Geschwindigkeit gefahrener Strecke werden mit den besten Werten im jeweiligen Bereich verglichen und wenn man diesen merklich überschreitet, wird der entsprechende Tipp gegeben. Der Vergleich mit anderen über das soziale Netzwerk erfolgt folgendermaßen: die Benutzer werden nach bestimmten Kriterien (wie Zustand der Straße, Fahrtdauer, Durchschnittsgeschwindigkeit, etc.) in Gruppen eingeteilt und nur innerhalb dieser Gruppe verglichen. Dieses Vorgehen wurde gewählt, weil beispielsweise eine Autofahrt in einer Stadt nicht direkt mit einer Fahrt auf einer Autobahn vergleichbar ist.

Das System wurde auf insgesamt 100 Testfahrten mit 5 Fahrgästen und 5 verschiedenen Fahrzeugtypen sowohl auf dem Highway wie auch im Stadtverkehr getestet. Dabei wurde ein positiver Einfluss auf den Spritverbrauch bewiesen.

2.1.3 Location-Based Challenges

Ecker et al. [7] haben ebenfalls eine Anwendung mit visuellem Feedback über ein Smartphone entwickelt. Diese basiert auf dem Prinzip von Echtzeit-Feedback gepaart mit einem Ranking über soziale Netzwerke. Der Fahrer muss auf seiner Strecke sogenannte "Challenges" bewältigen, die einen festen Start- und Endpunkt haben. Dadurch kann der eigene "Score" (Hauptkriterium: Spritverbrauch) leicht mit dem von anderen Teilnehmern verglichen werden, welche dieselbe Strecke gefahren sind. Die Anzeige auf dem Smartphone variiert je nachdem, ob das Fahrzeug steht (Eingabemöglichkeit und zusätzliche weniger wichtige Informationen) oder sich bewegt (für das Spiel essentielle Informationen, wie z.B. aktueller Spritverbrauch). Bei einer Studie mit 5 Testteilnehmern wurde das Handy im Zentrum des Fahrzeugs montiert. Die Testteilnehmer bestätigten einen motivierenden Einfluss der Anwendung (6.2 von 7 Punkten) und gaben an, Spaß an dem Spiel (6.4 von 7 Punkten) gehabt zu haben.

2.1.4 DriveGain

Tulusan et al. [13] haben eine Anwendung namens DriveGain untersucht, die von "DriveGain Ltd., UK" entwickelt wurde. Die Beurteilung des Fahrstils basiert auf korrektem Gangwechsel während Beschleunigung und Bremsvorgang und der optimalen Durchschnittsgeschwindigkeit (abhängig vom Fahrzeugtyp). Die Benutzeroberfläche zeigt unter anderem die Beurteilung dieser Parameter über die letzten Minuten, ebenso wie den empfohlenen Gang und die Gesamtpunktzahl der aktuellen Fahrt. Gemessen werden diese Eigenschaften durch GPS-Sensor und Beschleunigungsmesser am Handy. In einer Studie mit 50 Teilnehmern war der Kraftstoffverbrauch mit DriveGain im Durchschnitt um 3,23% weniger als in der Vergleichsgruppe ohne die Anwendung. Die Studie fand unter der besonderen Bedingung statt, dass sämtliche Testpersonen Berufsfahrer waren, also meist nicht selbst für die Spritkosten aufkommen müssen.

2.2 Das Hauptproblem: Ablenkung

Sämtliche besprochene Anwendungen erfordern "Mitdenken" und arbeiten hauptsächlich mit visuellem Feedback. Das stellt im Kontext des Autofahrens ein Problem dar, weil sich der Fahrer auf die Straße und seine Umwelt konzentrieren muss, um seine eigene und die Sicherheit seiner Mitmenschen gewährleisten zu können⁶. Rouzikhah et al. [10] führen einige Studien auf, die zeigen, dass Ablenkung und Unaufmerksamkeit zu erheblich erhöhtem Unfallrisiko führen. Sie unterteilen Ablenkung in vier verschiedene Arten:

1. Visuelle Ablenkung (der Blick wird von der Straße abgewandt und auf ein anderes Ziel gerichtet)
2. Akustische Ablenkung (das Gehör wird auf etwas anderes, als die relevante Umgebung gerichtet, beispielsweise auf Musik)
3. Physische Ablenkung (es wird eine für das Fahren irrelevante Tätigkeit ausgeführt, z.B. CD wechseln, statt Lenkrad halten)
4. Kognitive Ablenkung (die Gedanken des Fahrers konzentrieren sich auf etwas anderes, als das Autofahren)

In einer möglichen Eco-Driving-Anwendung haben wir beispielsweise eine Anzeige der bisher erreichten Punkte (1.), akustische Warnungen (2.), evtl. eine benötigte Eingabe (3.) und kognitive Ablenkung (4.) ist in jeder Art der Interaktion mit enthalten. Hinzu kommt, dass es sich bei einem solchen Spiel um ein sog "secondary task" handelt [1], d.h. es ist nicht essentiell für die Aufgabe "Auto fahren", somit auch weniger wichtig zu nehmen, im Vergleich zu beispielsweise der Geschwindigkeitsanzeige.

2.3 Möglichkeiten für Feedback

Ein Feedback System ist wesentlicher Bestandteil eines Spiels [9] und für Eco-Driving-Anwendungen im Auto gibt es dafür verschiedene Möglichkeiten. Im Folgenden werden diese genauer beleuchtet, vor allem im Bezug auf die Stärke der Ablenkung des Fahrers.

2.3.1 Feedback nach der Fahrt

Es gibt die Möglichkeit Feedback erst nach der Fahrt zur Verfügung zu stellen. Das Problem der Ablenkung des Fahrers wäre auf diese Weise komplett beseitigt. Es führt allerdings zu einem Konflikt mit dem Ansatz *Gamification*.

⁶<http://epp.eurostat.ec.europa.eu/portal/page/portal/transport/data/database>

Bei Spielen ist es wichtig, sofortige Meldung über erreichte Punkte oder gebrochene Regeln zu erhalten, damit die Motivation konstant hoch bleibt [9].

2.3.2 Echtzeit-Feedback

Für Echtzeit-Feedback während der Fahrt werden drei mögliche Formen unterschieden: Head-Down-Displays, ein Head-Up-Display und akustisches Feedback.

Head-Down-Display (HDD).

Unter dem Begriff Head-Down-Display fassen wir alle Displays zusammen, für die der Fahrer seinen Blick von der Straße abwenden muss: darunter fallen sowohl die Oberfläche eines Smartphones, als auch das Driver-Centered Combi-Display (DCD) und das Central Information Display (CID). Auf dem DCD werden in der Regel Motordrehzahl, Geschwindigkeit und Tankfüllung angezeigt, während das CID bisher für den Radio oder die Klimaanlage dient.

Ein Vorteil all dieser Head-Down-Displays ist, dass die Autofahrer sie bereits gut kennen, bzw. daran gewöhnt sind. Die beiden integrierten Displays gibt es in jedem Auto und wer ein Smartphone besitzt, ist an den Umgang mit diesem in der Regel auch gewöhnt. HDDs bieten auch unmittelbares Feedback, was dem Spiel-Charakter einer Anwendung sehr entgegen kommt. Damit sind wir aber auch bei dem großen Problem angelangt: um dieses Feedback zu erhalten muss der Fahrer den Blick auf das Display richten und somit von der Straße abwenden. Eine mögliche Verbesserung bieten hier die sogenannten Head-Up-Displays.

Head-Up-Display (HUD).

1988 gab es das erste HUD für den Automobilbereich bei General Motors, seitdem waren sie üblicherweise nur in der Luxusklasse vertreten, oder als zusätzliches Zubehör zu erwerben [14]. In der letzten Zeit scheint es sich jedoch in der Automobilbranche weiter auszubreiten (beispielsweise plant auch VW 2014 ein integriertes HUD im neuen Passat⁷).

Ein HUD macht es möglich, Informationen direkt in das Sichtfeld des Fahrers zu projizieren. Für diesen entsteht durch einen optischen Trick der Eindruck, das Bild würde einige Meter vor ihm über der Motorhaube schweben. Erstmals wurden solche Displays in den 70er Jahren für Kampfjets und tieffliegende Militärhelikopter eingesetzt, sicherheitstechnisch äußerst kritischen Systemen, vor allem bezüglich der Ablenkung des Piloten. In Autos wurden HUDs bisher hauptsächlich für essentielle Informationen genutzt, wie Geschwindigkeitsanzeige oder Warnungen [1]. Es gibt jedoch auch schon Studien, die die Brauchbarkeit für weniger wichtige Informationen testen [14].

Im Vergleich zu anderen Displays im Auto (allgemein Head-Down-Display HDD), wie dem Driver-Centered Combi-Display (DCD) für Geschwindigkeitsanzeige, Drehzahl, etc. oder dem Central Information Display (CID) für beispielsweise Klimaanlage oder Radio hat das HUD einige Vorteile. Sogenannte "Eye-Gaze-Studies", bei denen die Bewegung der Augen verfolgt wird belegen, dass beim Informations Ablesen von einem HUD die Blickdauer verkürzt ist [1]. In einer Studie von Charissis et al. [2] wird gezeigt, dass HUDs im Vergleich zu herkömmlichen Instrumenten-Panels die Reaktionszeiten von älteren Autofahrern verbessert und die Häufigkeit

⁷<http://www.autobild.de/artikel/vw-passat-2014-vorschau-4202187.html>

von Kollisionen wirksam verringert. Bezuglich der Akzeptanz beim Benutzer zeichnen Tests ebenfalls ein positives Bild: Der Großteil der Teilnehmer betont, dass sie sich beim Autofahren mit dem HUD sehr wohl fühlen [1] und im Vergleich zu Head-Down-Displays oder einem rein akustischen Display erreicht es die höchste Nutzerzufriedenheit [14].

Auch HUDs haben jedoch ihre Nachteile. Ablaßmeier et al. [1] beschreiben ein ungewolltes Abdriften der Aufmerksamkeit des Fahrers auf das Display (“Cognitive Capture”) oder das sogenannte “Tunneling”, ein Effekt, der die Ränder des Sichtfelds verschwimmen/verschwinden lässt und in manchen Studien wurde eine Fehleinschätzung von Entfernung beobachtet. Ein großes Problem stellt auch die Abhängigkeit von den Lichtverhältnissen dar, da ein hoher optischer Kontrast benötigt wird, um das Bild sichtbar zu machen.

Audio-Feedback.

Eine dritte Möglichkeit für Echtzeit-Feedback bietet ein akustisches Interface. Dicke et al. [4] haben ein System mit rein akustischem Feedback im Vergleich zu einem HUD, bzw. einem HUD mit zusätzlichem Audio-Feedback getestet. Dabei wurden verschiedene Aufgaben von den Testpersonen gefordert, bei denen sie durch diverse Menüs navigieren mussten. Das System mit Audio-Feedback kann die kognitive Ablenkung erheblich verringern. Im Vergleich zum rein visuellen Display war das Auftreten von Fahrfehlern bei den Testpersonen merklich verringert. Es hat sich jedoch auch gezeigt, dass es mit rein akustischem Feedback am längsten dauert, eine Aufgabe (Interaktion mit dem System) zu erfüllen und außerdem die dabei empfundene Arbeitsbelastung am höchsten ist.

3. FAZIT UND AUSBLICK

Gamification wirkt sehr vielversprechend, gerade im Bereich des Eco-Driving, das (im hier definierten Sinn) nur auf freiwilliger Basis funktionieren kann (siehe auch “freiwillige Teilnahme” als wesentliches Merkmal eines Spiels). Welche Art des Feedbacks die beste ist, ist eine Frage, die nicht so einfach zu beantworten ist: Feedback nach der Fahrt hemmt die Motivation, Audio-Feedback ist ineffizient und HDDs, aber auch HUDs sind als kritisch einzustufen, was die Ablenkung des Autofahrers betrifft. Im Moment erreicht ein HUD mit zusätzlichem Audio-Feedback die besten Nutzerbewertungen und ist bezüglich der Ablenkung vertretbar [4]. Vor allem im Hinblick auf die rasante Entwicklung von Systemen wie dem automatischen Spurhalten, automatischem Auffahr-Stopp oder generell dem Ansatz des “Piloted Driving”^{8 9} ist hier vielleicht auch einfach noch etwas Geduld angebracht, denn mit der Integration solcher Systeme nimmt die Schwere der kurzzeitigen Ablenkung im Bezug auf Sicherheit ab. Unter diesem Gesichtspunkt kann man sich jedoch auch fragen, ob die aufwändige Erforschung und Entwicklung von Systemen, die Einfluss auf den Fahrer nehmen

⁸<http://www.theengineer.co.uk/news/traffic-jam-technology-is-step-towards-autonomous-motoring/1015532.article>

⁹<https://www.audi-mediaservices.com/publish/ms/content/en/public/pressemittelungen/2013/01/29/handelsblatt-tagung.html>

noch sinnvoll ist. Schenkt man den Medien Glauben^{10 11}, so befinden wir uns auf dem besten Weg zu selbstständigen Fahrzeugen, die menschliche Kontrolle und Steuerung nicht mehr benötigen.

4. REFERENCES

- [1] M. Ablaßmeier, T. Poitschke, F. Wallhoff, K. Bengler und G. Rigoll. Eye gaze studies comparing head-up and head-down displays in vehicles. In *IEEE International Conference on Multimedia and Expo*, pages 2250–2252. IEEE, 2007.
- [2] V. Charissis, S. Papanastasiou, L. Mackenzie und S. Arafat. Evaluation of collision avoidance prototype head-up display interface for older drivers. In *Human-Computer Interaction. Towards Mobile and Intelligent Interaction Environments*, pages 367–375. Springer, 2011.
- [3] S. Deterding, D. Dixon, R. Khaled und L. Nacke. From game design elements to gamification: defining gamification. In *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, pages 9–15. ACM, 2011.
- [4] C. Dicke, G. Jakus und J. Sodnik. Auditory and head-up displays in vehicles. In *Human-Computer Interaction. Applications and Services*, pages 551–560. Springer, 2013.
- [5] S. Diewald, A. Möller, L. Roalter, T. Stockinger und M. Kranz. Gameful design in the automotive domain: Review, outlook and challenges. In *Proceedings of the 5th International Conference on Automotive User Interfaces and Interactive Vehicular Applications*, AutomotiveUI ’13, pages 262–265, New York, NY, USA, 2013. ACM.
- [6] R. Ecker, P. Holzer, V. Broy und A. Butz. Ecochallenge: A race for efficiency. In *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services*, MobileHCI ’11, pages 91–94, New York, NY, USA, 2011. ACM.
- [7] R. Ecker, B. Slawik und V. Broy. Location based challenges on mobile devices for a fuel efficient driving behaviour. In *Proceedings of fifth International Conference on Persuasive Technology, Copenhagen, Denmark*, 2010.
- [8] V. C. Magaña und M. M. Organero. Gafu: A game to save fuel using social networks. In *International Conference on Connected Vehicles and Expo (ICCVE)*, pages 151–157. IEEE, 2013.
- [9] J. McGonigal. Reality is broken. *Jonathan Cape, London*, 2011.
- [10] H. Rouzikhah, M. King und A. Rakotonirainy. Examining the effects of an eco-driving message on driver distraction. *Accident Analysis & Prevention*, 50:975–983, 2013.
- [11] R. M. Ryan und E. L. Deci. Intrinsic and extrinsic motivations: Classic definitions and new directions.

¹⁰<http://www.welt.de/debatte/kommentare/article128675822/Ist-das-die-Zukunft-unserer-Mobilitaet.html>

¹¹<http://www.zeit.de/zeit-wissen/2013/03/autonomes-autogoogle-fahrzeugindustrie>

- Contemporary educational psychology*, 25(1):54–67, 2000.
- [12] S. Siero, M. Boon, G. Kok und F. Siero. Modification of driving behavior in a large transport organization: A field experiment. *Journal of Applied Psychology*, 74(3):417, 1989.
 - [13] J. Tulusan, T. Staake und E. Fleisch. Providing eco-driving feedback to corporate car drivers: what impact does a smartphone application have on their fuel efficiency? In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, pages 212–215. ACM, 2012.
 - [14] G. Weinberg, B. Harsham und Z. Medenica. Evaluating the usability of a head-up display for selection from choice lists in cars. In *Proceedings of the 3rd International Conference on Automotive User Interfaces and Interactive Vehicular Applications*, pages 39–46. ACM, 2011.

Alternativen zu Passwort und Pin

Maximilian Steindl
Universität Passau
Innstr. 43
94032 Passau, Germany
maximiliansteindl@gmx.de

ABSTRACT

Biometrie könnte in naher Zukunft alle unsere Daten sicher vor unbefugtem Zugriff schützen. Es gibt zahlreiche Ansätze wie man biometrische Techniken sowohl auf dem Desktop Computer sowie auf mobilen Geräten realisieren kann. Die Vorteile von Authentifizierung, ohne sich dabei komplizierte Passwörter merken oder ständig auf Chipkarten achten zu müssen liegen auf der Hand, da lange Zeichenfolgen für die meisten Menschen nur schwer einprägsam sind. Speziell die Verhaltensbiometrie, die beim Tippverhalten angewandt wird, hat ein hohes Potenzial, um das herkömmliche Passwort abzulösen. Entscheidend ist dabei die hohe Zuverlässigkeit, die nur gering unter der des Iris - Scans liegt.

Außerdem punktet das Tippverhalten - Erkennungssystem aus datenschutzrechtlicher Sicht, weil eben nur ein gewisses Muster erzeugt wird, das verschlüsselt im System vorliegt und somit einem Angreifer nur wenig nützt. Neben diesem Verfahren gibt es noch weitere biometrische Techniken, die in den unterschiedlichsten Einsatzgebieten ihre Stärken haben und das Passwort ablösen können.

Keywords

Biometrie, Sicherheit, Authentifizierung

1. EINLEITUNG

Die Sicherheit eines herkömmlichen Passworts hängt stark von der Zeichenglänge, der Verwendung von unterschiedlichen Sonderzeichen sowie von einer möglichst zufälligen Reihenfolge der Zeichen ab. Diese Eigenschaft bringt allerdings den großen Nachteil mit sich, dass die Passwörter nur sehr schwer zu merken sind und leicht vergessen werden können. Aus diesem Grund legen viele Nutzer ein kürzeres und besser zu merkendes Passwort an, das aus Namen oder Geburtsdaten besteht[14]. Hierbei sinkt der Schutz der Passwörter enorm, weil Hack-Programme wie Brute Force oder Rainbow Tables systematisch Zeichenkombinationen auszuprobieren. Fehlen Zahlen oder Sonderzeichen in einem Passwort, so fällt die

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Advances in Embedded Interactive Systems '14 Passau, Germany
Volume 2, Issue 3 (October 2014). ISSN: 2198-9494

mögliche Anzahl an Kombinationen stark ab und das Programm muss wesentlich weniger Rechenzeit investieren, um den Schlüssel herauszufinden. Dies dauert bei den heutigen CPU Leistungen je nach Länge der Zeichen meist absehbar lange[10].

Außerdem werden heutzutage viele persönliche Applikationen wie Banking, E-mail oder Soziale Netzwerke auf mobilen End-Geräten synchronisiert. Das bietet für den Nutzer die Vorteile, dass er mit mehreren Geräten auf Apps zugreifen kann und die Änderungen bei allen Systemen übernommen werden. Allerdings bietet sich ein weiteres Angriffsziel um an fremde Daten zu gelangen. Bei fast allen Smartphones genügt ein einziger Login - Befehl um auf sämtliche Anwendungen Zugriff zu erhalten. Lässt man sein mobiles Gerät unbeachtet liegen oder wird es gestohlen, ist es für Angreifer relativ leicht sich Zugang zu verschaffen und persönliche Daten auszulesen. Aus diesen genannten Gründen verfolgen neuere Sicherheitsverfahren einen anderen Ansatz mit Hilfe von biometrischen Merkmalen von Benutzern.

2. BIOMETRIE

Im Gegensatz zu Authentifizierungsmechanismen, die auf persönlichem Wissen (Passwörter) oder auf dem Mitführen von Gegenständen (z.B. Chipkarte) beruhen, ist bei biometrischen Techniken keines der Beiden erforderlich. Biometrische Verfahren können jederzeit ohne, dass die jeweilige Person sich speziell darauf vorbereiten muss, wie zum Beispiel Wissen abrufen, angewandt werden.[2]

In der Literatur unterscheidet man zwischen impliziter und expliziter Authentifizierung. Hier wird im Wesentlichen die Art und Weise der Zutrittskontrolle unterschieden. Wenn ein System den Benutzer dazu auffordert, sich zu identifizieren, indem er zum Beispiel ein Passwort einträgt, so nennt man diesen Vorgang explizite Authentifizierung. Hingegen gibt es die implizite Form, bei der die Zugangskontrolle beliebig erfolgt. Hier wird der Nutzer zum Beispiel durch seine Gangart von Kameras erfasst, durch das System erkannt und ihm wird Zugang gewährt[15]. Letzterer Fall ist für den Benutzer mit weniger Zeitaufwand verbunden und die Benutzerfreundlichkeit ist wesentlich höher.

Bei der biometrischen Identifikation kann eine Person sowohl mit oder ohne deren Einwilligung erkannt werden bzw. die Merkmale der Person können erfasst werden[14]. Hierbei muss sorgfältig auf Datenschutz, Menschenwürde und das Persönlichkeitsrecht geachtet werden. Solange keine Zusätzlichen Informationen wie zum Beispiel der Name vorliegt, sind biometrische Daten jedoch als nicht-personenbezogen anzusehen. Sind Informationen der erkannten Person im Sys-

tem vorhanden, müssen diese Daten besonders gut geschützt werden[1].

Bei der Identifikation führt ein spezieller Algorithmus, je nach Art der verwandten Erkennungstechnik, Mustererkennung durch und gleicht dieses Muster wiederum mit den Datensätzen ab und prüft die Übereinstimmung.[5] Allerdings gilt bei der biometrischen Identifikation, dass Datensätze lediglich auf ihre Ähnlichkeit untersucht werden können. Aufgrund von Messabweichungen entstehen immer geringfügige Fehler, die dazu führen, dass die Messdaten nicht genau mit den Einträgen der Datenbank übereinstimmen[5]. Deshalb muss ein gewisser Toleranzrahmen eingerichtet werden, um dennoch Personen zuordnen zu können. Bei Passwort und Pin hingegen gibt es eine eindeutige Passgenauigkeit. Stimmt das eingegebene Passwort nicht exakt mit dem geforderten Passwort überein, so kann der Benutzer eindeutig abgewiesen werden.[1]

3. VORSTELLUNG AUSGEWÄHLTER VERIFIKATIONSARTEN

Um die Problematik, die Passwörter und Pins mit sich bringen, zu lösen bzw. wesentlich benutzerfreundlichere Authentifizierung zu ermöglichen, gibt es mehrere biometrische Ansätze. Bei diesen Techniken muss der Benutzer lediglich anwesend sein und in manchen Fällen simple Anweisungen befolgen, um die Zutrittskontrolle zu überwinden. Im Folgenden werden verschiedene biometrische Verfahren vorgestellt.

3.1 Fingerabdruck

Fingerabdrücke sind ein eindeutiges Merkmal, das bei jedem Menschen spezifisch ist und selbst bei einerigen Zwillingen deutlich unterschieden werden kann. Außerdem sind die Eigenschaften der Konstanz und der Einzigartigkeit ein sehr wichtiges Kriterium, um einen Fingerabdruck auf der Hand oder eingescannt in digitaler Form einem Menschen dauerhaft zuordnen zu können[11]. Diese Art der biometrischen Identifikation ist das am meisten verbreitetste Verfahren aufgrund der langen Tradition Verbreichensbekämpfung mit Hilfe von Fingerabdrücken zu unterstützen[14]. Bei den Abdrücken untersucht eine spezielle Software nach charakteristischen Merkmalen wie Bögen, Schleifen, Wirbeln, Abzweigungen, Anfangs- und Endpunkten an bestimmten Positionen (siehe Figure 1). Nachdem diese Punkte erkannt wurden, kann die biometrische Signatur ermittelt und ein Templatefingerabdruck erstellt werden, der später zum Abgleich dient. Die Qualität des Templates ist für die einwandfreie Funktion der Personenidentifikation entscheidend. Sowohl bei der Erstellung des Templatefingerabdrucks als auch bei der Aufnahme des Inputfingerabdrucks muss auf Sorgfalt geachtet werden. Verunreinigung oder zu starke Verdrehung beim Auflegen des Fingers kann eine Identifikation unmöglich machen [13].

3.2 Tippverhalten

Schreibmustererkennung zur Verifikation von Personen ist eine vergleichsweise junge Methode[14]. Jedoch bieten sich dabei entscheidende Vorteile gegenüber von Passwort und Pin. Zum Einen kann der Verifikationsvorgang kaum ausgespäht werden und zum Anderen ist diese Form von Identifi-



Figure 1: Fingerabdruck mit charakteristischen Punkten.¹

kation auch nicht übertragbar, was einen zusätzlichen Schutz liefert. Jede Person hat einen individuellen Schreibrhythmus, eine bestimmte Tippgeschwindigkeit, sowie eine erkennbare Beweglichkeit der Finger. Selbst ob man Links -oder Rechtshänder ist, kann beim Tippen erkannt werden. Diese Gegebenheiten können analysiert und ausgewertet werden. Daraus ergibt sich ein einzigartiges Schreibmuster, das immer wieder bei der Zugangskontrolle abgeglichen werden kann. Spezielle Hardware ist bei diesem Vorgang nicht notwendig, die herkömmliche Tastatur von Desktop PCs oder von Laptops reicht vollkommen aus, weil bei dieser Art von Verifikation der gesamte Vorgang in einer Software implementiert ist.[3] Möchte sich nun jemand in das System einloggen, so muss ein eigens gewählter Satz über die Tastatur eingegeben werden, diesen wertet die Software aus und vergleicht die Werte mit denen der Datenbank. Stimmen beide überein, wird Zugang gewährt. Andernfalls wird der Benutzer abgelehnt.

Allerdings gibt es auch kritische Ansätze bei diesem Verfahren. So kann zum Beispiel keine richtige Zugriffskontrolle stattfinden, wenn sich ein Benutzer an der Hand oder an den Fingern verletzt hat, da der übliche Schreibfluss verändert werden kann. Außerdem ist die Authentisierung für jüngere Personen, die sich noch an keinen eigenen Schreibstil gewöhnt haben möglicherweise unmöglich. In diesen Fällen muss auf die Verwendung von Passwörtern oder alternativen Verfahren zurückgegriffen werden.[14]

3.3 Tippverhalten auf mobilen Geräten

Ähnlich wie bei der Tipperkennung auf einer Tastatur, gibt es die Möglichkeit auf mobilen Geräten, die über einen Touchscreen verfügen, eine Benutzererkennung durchzuführen. Grafische Authentifizierungsschemata, wie sie aktuell in Android Handys angewandt werden, können gegenüber numerischen Passwörtern von den Anwendern leichter gemerkt werden. Bilder lassen sich besser einprägen als komplizierte Buchstaben -und Zahlenfolgen[10].

Um ein Gerät zu entsperren, muss ein fest definiertes Muster, das aus Linien zwischen bereits vorhandenen Punkten besteht, mit den Fingern auf das Display gezeichnet werden. Das Verfahren steigt also bedeutend die Benutzerfreundlichkeit, allerdings sinkt die Sicherheit stark hingegen numerischen Passwörtern. Das eingegebene Muster kann leicht ausgespäht oder manchmal sogar auf dem Display abgelesen werden, da die Fettschlieren deutliche Spuren hinterlassen und Aufschluss auf das Entriegelmuster geben können. Deshalb gibt es weiterführende Arbeiten um das Konzept der grafischen Authentifizierung weiterentwickeln[7]. Hier fin-

¹Figure 1 aus <http://www.nationwidecreditexposed.com/wp-content/uploads/2013/03/The-Fingerprint-Recognition.jpg>

det wieder eine verhaltensbiometrische Verifikation als unterstützende Technik Anwendung. Der bereits vorhandene grafische Entsperrungsvorgang bleibt erhalten und wird zusätzlich durch eine Eingabemustererkennung erweitert (vgl. Tippverhalten). Mittels Touchscreen können ausgeübter Druck auf das Display, Größe der Finger, Eingabegeschwindigkeit uvm. während der Entrieglung erfasst und ausgewertet werden. Ein spezieller Algorithmus führt diese Rohdaten in ein Muster über. Danach lässt sich durch Abgleichen des Eingabemusters mit dem Referenzmuster feststellen, ob die Nutzung zulässig ist.[7]

Zu dieser Arbeit gibt es bereits Studien, die dieser Methode durchaus Potential bescheinigen. Die richtige Erkennung eines rechtmäßigen Nutzers ist relativ hoch bei ungefähr 90%, allerdings wird einem unrechtmäßigen Benutzer in jedem zweiten Fall der Zugang gewährt. Die Studie zeigt, dass Ansätze mit aktiver Verhaltensbiometrie durchaus auch auf mobilen Geräten umsetzbar sind, aber zum jetzigen Zeitpunkt ist die Entwicklung noch nicht weit genug fortgeschritten, um sie zweckmäßig einzusetzen zu können. Sinkt die Falscherkennungsrate deutlich nach unten und es wird unrechtmäßigen Benutzern kein Zutritt mehr erteilt, so kann diese Weiterentwicklung zur Sicherung mobiler Geräte beitragen [7][12][9].

3.4 Iriserkennung

Die Iriserkennung ist ein sehr zuverlässiges Verfahren zur biometrischen Identifikation, das seit einiger Zeit auch bei Hochsicherheitsbereichen verwendet wird[14]. Dieses Verfahren erfüllt alle Eigenschaften, die notwendig sind, um eine sichere Verifikation zu gewährleisten. Die Iris ist ein stabiles Merkmal, das heißt, wenn keine Verletzungen auftreten, bleibt das typische Irismuster eines jeden Menschen gleich. Dies liegt darin, dass die Iris als inneres Organ unter der Hornhaut des Auges liegt und zusätzlich noch durch die Augenlider geschützt wird.

Außerdem ist das Irismuster bei jedem Menschen spezifisch und kann unterschieden werden. Die Pigmentation ist zwar genetisch bedingt, aber das Muster einer Iris bildet sich zufällig aus. Deshalb sind auch Zwillinge anhand ihrer Irismuster klar unterscheidbar und selbst das Augenpaar eines einzelnen Menschen ist unterschiedlich[8].

Zusammenfassend ist wichtig, dass jeder Mensch über die zu erkennende Grundlage in diesem Fall die Augen verfügt, sie sind bei jedem Menschen unterschiedlich und über lange Zeit hinweg konstant.

Bereits 1993 wurde von John Daugman ein Algorithmus zur Iriserkennung entwickelt und wird auch heute noch in vielen Anwendungen eingesetzt. Der Identifikationsvorgang lässt sich in vier wesentliche Schritte unterteilen. Als erstes wird ein Bild des Auges aufgenommen. Daraus werden im nächsten Schritt alle überflüssigen Informationen entfernt. Hier wird die Iris aus dem Bild herausgefiltert und die restlichen Teile wie Pupille, Sclera sowie das Augenlid können gelöscht werden (siehe Figure 2 und 3). Jetzt kann das Muster der Iris in ein digitales Format umgewandelt werden. Im letzten Schritt findet, wie bei fast allen Erkennungstechniken, der Abgleich mit den Messdaten und den abgespeicherten Daten statt. Passen nun Beide mit hoher Wahrscheinlichkeit überein, so ist die Erkennung erfolgreich. Die Schwellwerte lassen sich nach Belieben regulieren, je nach Bedarf kann man sie heruntersetzen um das System sicherer zu machen, läuft jedoch Gefahr eine berechtigte Person abzuweisen.

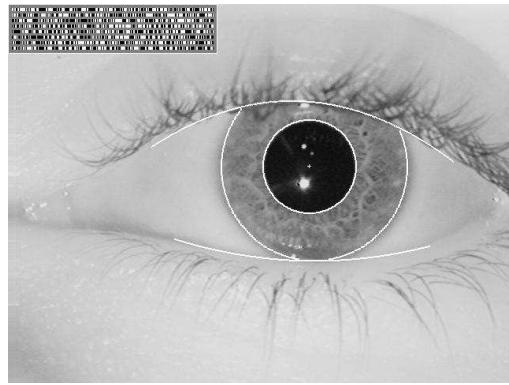


Figure 2: Die Iris mit dem dazugehörigen Code oben links[8].

Das Verfahren arbeitet sehr zuverlässig und bietet eine gute Lebenderkennung da sich die Pupille bei viel Licht zusammenzieht. Dieses Verhalten kann bei dem Identifikationsvorgang mit Veränderung der Lichtverhältnisse beobachtet werden. Als Nachteil muss der hohe Preis für die notwendige Hardware aufgeführt werden[8][14].

3.5 Retinascan

Neben dem Iriserkennungsverfahren gibt es noch ein weiteres Scanverfahren des Auges und zwar das der Retinamustererkennung. Bereits 1985 war es mit einem Gerät möglich die Blutgefäße hinter der Netzhaut (Retina siehe Figure 3) mit Hilfe eines Infrarot-Lasers aufzunehmen. Auch bei dem Blutgefäßmuster der Netzhaut gilt ihre Einzigartigkeit und kann dadurch sehr gut zur Unterscheidung von Personen eingesetzt werden. In etwa 400 charakteristische Punkte können der Aufnahme entnommen werden und in Templates der Größen zwischen 40 und 96 Bytes gespeichert werden. Das gesamte Verfahren wird als sehr überwindungsresistent eingestuft, da weder Bilder noch Augenatrappen das System überlisten können. Durch diesen großen Sicherheitsfaktor ist diese Technik bei Hochsicherheitseinrichtungen eine gefragte Methode, um für eine funktionierende Zutrittsicherung zu sorgen.[1]

Während der Messung muss eine Person für ca. 1,5 Sekunden im Abstand von 1-2 cm vor der Aufnahmeeoptik ruhig verweilen. Währenddessen bemerkt der Nutzer ein rotierendes grünes Licht, allerdings nicht das Infrarotlicht, das die tatsächliche Messung bzw. die Bildaufnahme des Adernmusters der Retina aufnimmt. Dieses Muster dient zum Abgleich der Datenbank.

Die Tatsache, dass ein Laser durch das Auge auf dessen hinterste Schicht trifft, löst bei vielen Nutzern die Angst vor Schäden am Auge aus. Auch die Position des Messapparats unmittelbar vor dem Auge bestärkt die Vorbehalte gegen diese Verifikationsart. Außerdem muss für die Messung aufwendige Spezialtechnik eingesetzt werden, die einen hohen Preis hat. Diese Punkte verhindern eine schnelle Verbreitung der Retinazutrittsicherung. [14]

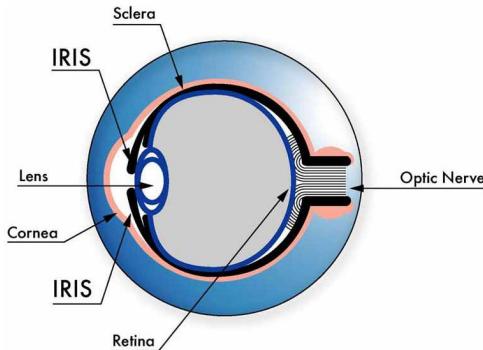


Figure 3: Die Positionen der Iris und er Retina im Auge².

3.6 Gesichtserkennung

Menschen nutzen am häufigsten diese biometrische Methode zur Erkennung von Personen. Nebenbei werden jedoch unbewusst noch weiter Merkmale wie Größe und Statur bemerkt, die zur Erkennung beitragen. Ein maschinelles Verfahren kann hingegen nur aus dem Bild des Gesichtes Informationen gewinnen, was die Aufgabe erschwert.[6]

Seit 2005 findet man biometrische 2-D-Gesichtsbilder als digitales Format auf Reisepässen von EU-Bürgern, um die Grenzkontrollen zu unterstützen.[6] Mit dem staatlichen Interesse für biometrische Erkennungssysteme steigerte sich der Anreiz der Weiterentwicklung von Gesichtserkennung stetig.[4]

Bei der Gesichtserkennung kommen sowohl zwei- als auch dreidimensionale Verfahren zum Einsatz. In beiden Bereichen dient die Geometrie der Gesichtsoberfläche als Verifikationskriterium. Zweidimensionale Gesichtserkennung Bei der zweidimensionalen Gesichtserkennung kommen Foto- oder Videokameras zum Einsatz, die eine sehr gute Bildqualität versprechen. Für ein aussagekräftiges 2-D-Bild bedarf es der Einhaltung folgender Kriterien: Das Bild muss etwa zu 70% durch das Gesicht ausgefüllt sein. Das Gesicht sollte neutral im Ausdruck sein und darf durch Haare oder eine Brille in keiner Weise verdeckt sein. Frontalaufnahme, gute Beleuchtung und Schärfe verstehen sich von selbst. Das Problem dabei liegt auf der Hand: „Die Einhaltung all dieser Kriterien sowohl bei der Aufnahme des Referenzbildes (Passausstellung) als auch beim späteren Vergleich (bei der Grenzkontrolle) ist schwer herzustellen [...].“ Nur in den seltensten Fällen stimmen alle Parameter überein. Außerdem ist die sog. Lebenderkennung bei diesem System noch nicht ausgereift genug, d.h., die Sensoren können nicht unterscheiden, ob wirklich ein Mensch vor ihnen steht oder ob es sich um ein ausgedrucktes Foto oder ein abgespieltes Video handelt. Das System ist also nicht in der Lage, ohne Überwachung eines Kontrolleurs zu arbeiten. Dreidimensionale Gesichtserkennung Die dreidimensionale Vermessung des Gesichts ist eine Erweiterung der 2-D-Aufnahme um eine dritte Dimension. Der Abstand zwischen Sensor und Gesichtsprofil kann bestimmt und daraus eine Tiefeninformation berechnet werden. Damit ist es möglich, eine komplette Gesichtsgeometrie einer Person herzustellen. Um das Ergebnis noch zu verfeinern, wird an jedem Oberflächenpunkt zusätzlich eine

²Figure 3 aus <http://static.ddmcdn.com/gif/biometric-1.jpg>

Farbinformation gezogen. Beim Abgleich von Referenzmodell und 3-D-Bild müssen die Modelle identisch ausgerichtet werden. Das ist über die sog. Landmarken des Gesichts (Augenwinkel, Nase, etc.) möglich. Ein enormer Vorteil gegenüber 2-D-Bildern ist, dass die 3-D-Modelle immer metrisch korrekt sind. Das bedeutet, bei zweidimensional aufgenommenen Bildern führt ein variiernder Abstand zur Kamera zu unterschiedlich großen Bildern. Bei einer 3-D-Aufnahme bleiben die Grundmaße erhalten. Der Augenabstand beispielsweise nimmt durch eine verzerrte Aufnahme keine anderen Maße an. Da bei der 3-D-Gesichtserkennung deutlich mehr Informationen vorliegen, kann auch detaillierter unterschieden werden. Die Wahrscheinlichkeit von Falsch-Akzeptanz-Fehlern kann dadurch rapide gesenkt werden .[6]

4. FAZIT

Schon heute gibt es weit erforschte Techniken, die einen wirksamen Schutz vor unbefugten Zutritt bieten.[16] Speziell die Iriserkennung funktioniert sehr gut und kann das Passwort dauerhaft ablösen, allerdings müssen die Preise für die notwendige Hardware noch weiter fallen, damit diese Technik auch im privaten Sektor für Nutzer bezahlbar wird.

Auf mobilen Geräten gibt es die Optionen mit Fingerabdruck oder Tippverhalten das Gerät zu entriegeln. Hierbei ist die Entwicklung allerdings noch in der Anfangsphase und muss noch weiterentwickelt werden um von der Gesellschaft akzeptiert zu werden.

5. REFERENCES

- [1] F. M. Abbühl and D.-I. P. K. Bittner. Datenschutzrechtliche aspekte bei der aufnahme biometrischer merkmale in ausweispapiere. 2004.
- [2] A. Albrecht. Authentizität im elektronischen rechtsverkehr und persönlichkeitsschutz beim einsatz biometrischer verfahren. In *BIOSIG*, pages 129–138, 2003.
- [3] D. Bartmann and C. Breu. Eignung des biometrischen merkmals tippverhalten zur benutzerauthentisierung. 2004.
- [4] D. Baur. Automatische gesichtserkennung: Methoden und anwendungen. *München. Online verfügbar unter http://www. medien. ifi. lmu. de/fileadmin/mimuc/hs_ws0506/papers/ Automatische_Gesichtserkennung. pdf*, zuletzt geprüft am, 27:2011, 2011.
- [5] M. Behrens and R. Roth. Grundlagen und perspektiven der biometrischen identifikation. In *Biometrische Identifikation*, pages 8–26. Springer, 2001.
- [6] C. Busch and A. Nouak. Das eu-projekt 3d face-3d-gesichtserkennung für die unbeaufsichtigte grenzkontrolle. *Tagungsband zum*, 10:199–212, 2007.
- [7] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. C. Van Oorschot. Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism. *Dependable and Secure Computing, IEEE Transactions on*, 9(2):222–235, 2012.
- [8] J. Daugman. How iris recognition works. *Circuits and Systems for Video Technology, IEEE Transactions on*, 14(1):21–30, 2004.

- [9] A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann. Touch me once and i know it's you!: Implicit authentication based on touch screen patterns. In *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems*, pages 987–996. ACM, 2012.
- [10] D. Fox. Mindestlängen von passwörtern und kryptographischen schlüsseln. *Datenschutz und Datensicherheit-DuD*, 33(10):620–623, 2009.
- [11] P. Gupta, S. Ravi, A. Raghunathan, and N. K. Jha. Efficient fingerprint-based user authentication for embedded systems. In *Design Automation Conference, 2005. Proceedings. 42nd*, pages 244–247. IEEE, 2005.
- [12] M. Jakobsson, E. Shi, P. Golle, and R. Chow. Implicit authentication for mobile devices. In *Proceedings of the 4th USENIX conference on Hot topics in security*, pages 9–9. USENIX Association, 2009.
- [13] S. Jeyanthi, N. U. Maheswari, and R. Venkatesh. Implementation of biometrics based security system with integrated techniques. In *Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology, CCSEIT '12*, pages 37–42, New York, NY, USA, 2012. ACM.
- [14] C. Paulsen, K. Brunnstein, and H.-J. Mück. *Risikoanalyse Von Biometrischen Systemen*. PhD thesis, diploma thesis, supervisor: K. Brunnstein, AGN, Department of Informatics, University of Hamburg, 2003.
- [15] T. Stockinger. Implicit authentication on mobile devices. Media Informatics Advanced Seminar on Ubiquitous Computing, 2011.
- [16] M. Sujithra and G. Padmavathi. Next generation biometric security system: An approach for mobile device security. In *Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology, CCSEIT '12*, pages 377–381, New York, NY, USA, 2012. ACM.

Wearable Computing: Smart Watches

Sebastian Witt
Universität Passau
94032 Passau, Germany
witt09@stud.uni-passau.de

ABSTRACT

Mechanical watches have been our daily companion for a long time. They have given us access to date and time information anywhere and at any time. The invention of cellphones and especially smart phones changed the people's way of life, as it is possible to do a lot with a modern phone, from taking pictures or managing personal information right up to doing business. Smart watches instead are relatively new and still less popular than phones. However, there are domains where smart watches can be a helpful and life-improving gadget. This paper deals with the topic of smart watches, regarding general application design criteria and domains where these devices could be used. Furthermore, we discuss limitations and present current projects and advances.

Keywords

Second screens, Quantified self, Ubiquitous computing, Wearables

1. INTRODUCTION

Presenting date and time information everywhere, wrist-worn watches were an important companion for people's lives. Comparing them today is not as easy as ten years ago when they were only mechanical devices. Scientific and technological progress contributed to create small and powerful appliances. Smart watches are one of them. Combined with a smart phone, they do not only let the user know what time it is. They also provide instant access to information about the weather, messages or missed calls, like for example the Pebble watch¹ or the Sony SmartWatch². Other ones, like Basis³, contain accelerometers, temperature sensors and heart rate monitors for quantified self-tracking

¹<http://www.getpebble.com/>

²<http://www.sonymobile.com/gb/products/accessories/smartwatch/>

³<http://www.mybasis.com/>

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Advances in Embedded Interactive Systems '14 Passau, Germany
Volume 2, Issue 3 (October 2014). ISSN: 2198-9494

[21]. That means the sensors of such electronic devices collect data about one's activities in daily life. After analysing and evaluating them, the results are used to improve health or personal productivity, for instance [2]. Using the watch as a smart home controller in particular or to interact with one's environment in general goes a step further [4, 5]. We see there are various scenarios where we could use them in daily life, but so far they are still less pervasive than smart phones.

In this paper I would like to give an overview on the topic of "smart watches", starting with drawbacks like hardware limitations, short battery life and interaction difficulties due to the small size. Afterwards I talk about the various applications and domains where a smart watch could be used despite those limitations to make life more comfortable. This explains why it might be a helpful device for visually impaired or elder people. To complete this work, I present some recent research projects that develop new ideas or improve some of those depicted in the following.

2. LIMITATIONS

Although the first smart watches were invented about 15 years ago [15] and many others have followed since [21], a number of issues remains which mainly result from the size of the watch.

People wear it on their wrists, so the form factor requires a small screen size and only allows little space for input devices and batteries [15]. Therefore, achieving acceptable battery life while maintaining computational abilities results in a trade-off difficult to manage, as keeping energy consumption to a minimum requires efficient components.

Developing self-sustaining electronic devices, like self-winding mechanical watches for example, has been difficult to accomplish so far. As users are not accustomed to charge their watch as often as their smart phone or other devices, obtaining an acceptable battery life is desirable [9]. Using a larger capacity battery could solve that problem, but with a bigger battery the small form factor could not be achieved yet. Replacing an empty one would also be tricky due to the watch's size [9].

Second, battery life depends on software and usage, as the watch is either in sleep or active mode [9]. When not used, the watch only displays the current time. A study showed that the representation of an analog clock needs less pixels of the display than that of a digital clock. Besides lower energy consumption it also provided a better readability. Thus, the reduction of pixels needed for fonts, icons and graphics while maintaining a good legibility is intended [9].

This points to a further problem regarding usability, range of functions and interaction with the watch. Most current smart watches offer a mix of virtual screen and physical buttons. The small size limits the available interactive surface so occlusion and the so-called “fat-finger problem” reduce the interaction with the small screen and buttons [17]. Furthermore, information is mainly represented with small fonts, so especially for elder or visually impaired people the handling can be restricted [1]. Consequently, input methods and application fields are limited by the watch’s size. Therefore, contrary to smart phones, an increase in screen size to display more information and afford easily interaction is not possible [10]. Among others, Section 3.5 shows recent studies about how to improve input methods.

3. APPLICATIONS AND DOMAINS

Traditionally, watches are worn to access date and time information anywhere and anytime. Nowadays, smart watches are more than pure notification devices, as they are able to interact with the user and their environment. The following presents design criteria that should be considered when developing a smart watch, as well as different domains where these gadgets can be a helpful companion.

3.1 Application design criteria

Smart watches are able to do a lot more than display time or play an alarm sound to wake people up [15]. Today these gadgets provide instant notification of incoming calls, messages or e-mails using Bluetooth to connect to a smart phone [21]. The ability to connect with other, more powerful devices is an important aspect. The quantified self-tracking watch Basis is an example for it. Its integrated sensors record the data which a computer processes later on. This allows the use of low-power hardware and therefore saving energy is possible [21].

Surveys showed that people would like to manage personal information, access data from the web or have the ability to play music or games on their watch [15]. In order to ensure usability, the selection of input methods is important. However, a weighting of advantages and drawbacks has to be made. A keyboard is problematic because of the small interactive surface and few physical buttons. A touch screen is more versatile, but the interaction with a finger reduces the input area to four or five zones [15]. Scrolling through content can be an important feature, too, but might be difficult on a small touch interface. A roller switch and a rotating bezel, like in IBM’s Linux Watch [14, 15], seem like apt ways to implement it. Section 3.5 presents some recent projects that deal with interaction improvement, especially in terms of text input methods. Lyons et al. [11] present another approach to avoid those problems. Facet is a multi-display watch with multiple, independent touch-sensitive screens. That means a user can put each application in a separate screen or he extends an application to a number of screens. For instance, he maps the messaging app to one display and a social network stream to two others. Therefore arranging the applications and screens in an intelligent way, information and notifications are instantly visible to the user.

Voice recognition would be another possibility, interacting via microphone and speaker with the watch. However, it might be difficult to handle in some situations. This could be either due to bad voice recognition in a crowded or noisy environment [19] or to social problems. Studies showed that

people have privacy concerns and feel uncomfortable in society when they have to use a screenreader or other assisting devices, as they do not want to draw attention or curiosity from others [22].

3.2 Gesture recognition, eyes-free interaction

So far, we have discussed the functions of commercial or well-known smart watches. Studies showed that these devices are not only useful for displaying information or notifications. Hence, the following part deals with gesture recognition and eyes-free interaction on smart watches.

In [13], Morganti et al. developed a watch that focuses on the recognition of tagged objects as well as forearm, finger and hand gestures by using multiple technologies like radio frequency identification (RFID), inertial sensors or measuring the force in the wearer’s wrist. Approaches, studies and tests to evaluate the functionality are explained more detailed in their paper.

[16] presents the prototype of a wristwatch with haptic feedback. It receives information from a connected companion mobile device by using eyes-free gestures and returns a haptic stimulus with the assistance of a piezoelectric actuator. The motivation of this project are situations where acquiring information or changing the settings from a mobile device is difficult, noticeable or time consuming. As a concrete usage scenario the developers chose a conference. The speaker’s mobile phone is located at his seat with a “ringing profile”. He wants to switch to silent mode without interrupting his talk. With the help of his smart watch he can perform a gesture that changes the profile on his phone without having to walk to his seat. Therefore, Pasquero et al. [16] investigated three different categories of gestures. First, the device initiates an event or notification the user needs to respond [16]. Second, the user performs an action that changes the state of his device [16]. Third, the user requests information from the device, for instance whether he has some unread text messages or not [16]. Their experiments showed that in about 97% of the time, participants were able to receive notifications from the device, but only 73% could tell the exact number of pulses the watch made. This points to the problems Pasquero et al. faced. On the one hand, every participant has a different subjective perception. On the other hand, the required sensors differ in their degree of precision and repeatability, as they should remain small, powerful and cheap [16].

Bieber et al. [3] go a step further. They created a prototype watch using gesture recognition, so that a technician is able to control a digital manual on his Android pad hands-free during a complex assembly or maintenance work, as gloves and dirty fingers prohibit the interaction with a touch-screen interface.

[17] takes the wristband as an extended interaction surface. As it is a complement to the touch-screen based interaction, two actions are evaluated: pointing and sliding (Figure 1). Like mentioned in Section 3.1, scrolling can be difficult on a small screen due to visual occlusion. The wristband shape is suitable for those actions, as studies have shown. Meanwhile the display always stays visible. Using the surface of the wristband simplifies the scroll-gesture. Instead of moving the whole forearm, the user only has to move his thumb. The results of this test were compared with the action of absolute pointing. That means a list is mapped to the wristband so that the user can choose a certain area

from the list on it. A pilot study with the WatchIt prototype [17] showed that simple pointing and sliding gestures on the wristband had a high degree of usability. In about 90% of the time participants were able to select the correct item in a list. Sometimes, the attenders mixed up pointing and sliding, resulting in wrong signals as their finger skipped along the surface [17].

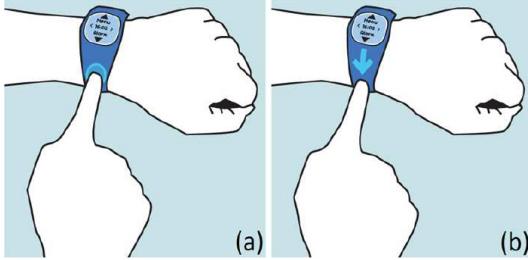


Figure 1: Interacting with the wristband using simple gestures: (a) pointing and (b) sliding on the internal strap with one finger. Adapted from [17].

3.3 Activity recognition

As stated in [2], current smart watches allow permanent monitoring of physical activities. The collected data can be used for various purposes, for instance safety or fitness applications. The data analysis is either made by the smart watch itself or on a smart phone [2]. In doing so, the phone wirelessly receives data from the watch, evaluates them and sends it back to the watch. Using this method results in a better battery life as no powerful hardware is necessary. Furthermore it is possible to associate the recorded data with the user's daily life. Communicating with peripherals is key here. [20] and Figure 2 give an example of activity recognition and self-tracking: A user arrives at his house and presses the door lock button to enter. The door lock wakes the watch and checks the user's ID. If it is registered, the door opens. While moving around the house, the watch periodically wakes up and sends its ID to a stationary node. On the one side it exposes its presence and on the other side it retrieves information about the location and activities from the nodes and peripherals. When the user measures his weight, his watch receives the activity from the body scale and shows a message from a smart pill reminder. Hence, the user goes to his bedroom to take the pills and presses a button afterwards to tell the watch the task is completed. Finally, he can send the recorded data to a tertiary service, like a smart phone for instance, in order to see, share or evaluate them.

Activity recognition demands reliable sensor information, especially from the acceleration sensor, as it is the most important one in this domain [2]. Differentiating between application fields like activity monitoring for health and fitness applications, inactivity recognition or gesture recognition is a challenge, as every field reveals different sensor requirements [2]. Some watches also provide an integrated light sensor that indicates whether artificial or sunlight is ambient. Using the light conditions surrounding a person helps to estimate her activity state. However, this can be difficult in every day life, as people sleep for instance in front of the television at night by a full light condition, or the sensor is

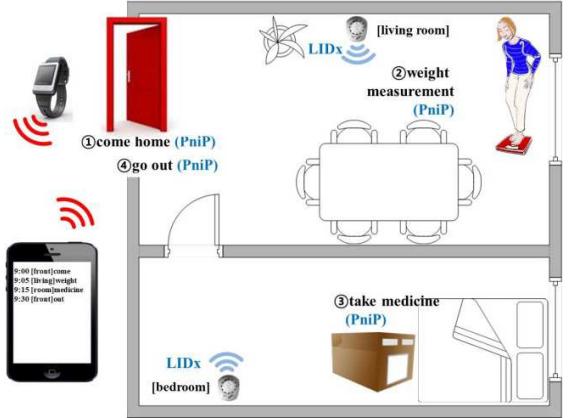


Figure 2: A watch based activity recognition and self-tracking scenario [20].

occluded by clothing, for instance. As a consequence, the detected light is different to the real light condition. These are points that make it difficult to estimate the person's activity state by measuring the surrounding light conditions [2].

3.4 Life-enhancing gadget

Several researches investigated the smart watch as a life-enhancing tool [1, 3, 19]. Especially elder or visually impaired people face problems with the small touch surface and buttons. Angelini et al. [1] propose a bracelet for older adults that combines health monitoring functions with a non-medical design and applications to facilitate everyday indoor and outdoor activities. Examples for this would be digital payment for shopping and transportation, health monitoring and alerts, as well as multimodal interaction with home appliances. In this case multimodal means providing visually impaired people with alternative ways to access technology. Perceptual capabilities like acoustics or speech are used to facilitate human interaction with computers. Therefore a black and white electronic-ink screen displays the information in form of visual notifications. This reduces reflections caused by sunlight and ensures high contrast. Moreover, simple vocal messages and haptic feedback assist the notifications. Actions like confirming a payment are performed on a single large touch surface, facilitating interaction.

Visually impaired people often rely on screen readers and voice commands. However, in some situations people are unable to pay attention to the reader for safety reasons or when voice command recognition is difficult because of a noisy environment [19]. In [19], they present a prototype system that uses a mixture of smart phone and smart watch for assisting low vision people in daily life. The screen interface is simplified like in [1]. To perform an action, the user taps on the screen to awake the watch and selects a function through arm gestures. The linked smart phone receives the watch's sensor data and uses its own camera for a vision-based detection task, providing the result of it through vibration feedback. Detecting wet floor signs automatically and warn the user with vibration feedback, as well as identifying specific symbols to assist the user in sev-

eral scenarios by using the smart phone's camera are tested with their prototype. A more specific and technical view in terms of implementing the so-called "vision-based modules" is given in [19].

Fall detection and monitoring daily activities allow the smart watch to be an appliance for assisted living, too, as the device is constantly in contact with the user [3]. One the one hand, it is a remembrance and confirmation aid. Reminding a person to take her medicine like in the scenario in Section 3.3 and Figure 2 is an example for it. On the other hand, using the technology of micro-electromechanical systems like accelerometers and gyroscopes, for instance, allow the detection of fall events [8]. Therefore, medical treatment can be provided in time and the level of injuries reduced [8]. Hsieh et al. [8] took two smart watches each with a three-axis gyroscope and an accelerometer to reduce false alarms when clapping, sitting or lying down. As a result, they achieved an accuracy of 95% in their experimental results. However, wearing two devices on both hands is unprofitable, hence they try to only use one for fall detection.

3.5 Recent works

The previous sections talk about design criteria and domains. Other than that, there are projects that try to improve the interaction with the small screen. Knibbe et al. [10] present a first attempt to extend the interaction area of the watch to the back of the wearer's hand. Using his fingers, hand and forearm for tapping or gesturing enables the user to perform certain actions, like zooming within a map or scroll through web-pages. While avoiding occlusion, it also provides a larger interaction space.

[6, 7] both deal with the improvement of text input on those little devices, because on-screen keyboards require larger space and the screen gets easily occluded while tapping. Therefore Funk et al. [7] developed a touch-sensitive wristband with vertical representation of the characters (Figure 3.a), whereas Dunlop et al. [6] split the screen into six zones, where every zone represents certain characters (Figure 3.b). A user study in [7] shows that participants achieved high performance with the proposed multitap layout. Using the screen with different zones also performed well, but revealed two problems of the prototype [6]. Firstly, the screen was unresponsive to fast repeated taps on the same area. Secondly, the layout needs some further investigations, as for instance a delete key was missing. Furthermore, users try to tap the actual latter rather than the large button, so it was not obvious that a group of characters forms a single button [6].

4. DISCUSSION

Although smart watches have experienced diverse development, there are still some issues that need to be solved in further works.

One thing is that many research teams that dealt with gesture recognition created their own set of gestures. Besides a waste of money and time it limits the progress of development, as most of the gestures to be recognized are similar [18].

Furthermore, security and privacy concerns are big topics today. As people wear watches mainly on their wrist, the display oriented outside, there might be a deficit in protecting personal information. Only few projects have addressed this problem so far, as mainly the security of the devices

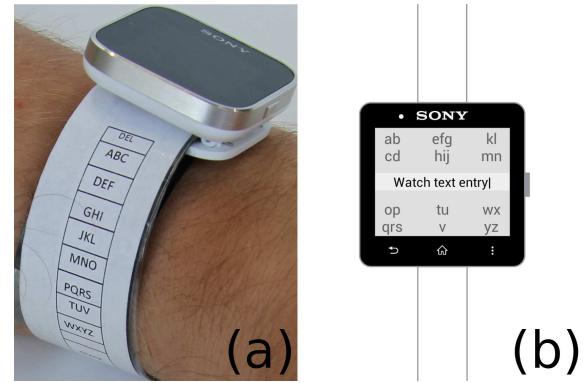


Figure 3: Text input improvement prototypes: (a) multitap layout keyboard, (b) screen split into zones. Adapted from [6, 7].

themselves or the privacy of produced data were regarded in former works [12].

At last, as already mentioned in Section 2, battery life is a main concern smart watches are still facing. Low computational requirements reduce power consumption a lot. However, they are then dependent on other devices for further processes. Achieving acceptable duration while maintaining computational abilities should be the way to go in the near future.

5. CONCLUSION

This paper gives insight into the latest state of the art regarding smart watches, primarily in terms of limitations, design criteria and different application domains. Unlike smart phones, watches are directly attached to the human body [3]. Therefore, monitoring activities and recognizing gestures make them more than only a second screen for providing notifications from a connected device. Despite their limitations in hardware and size, they are able to improve day-to-day activities, as pointed out above. Although many watches are still in development stage, their experiment results are promising and existing problems could be solved by doing further research.

6. REFERENCES

- [1] L. Angelini, M. Caon, S. Carrino, L. Bergeron, N. Nyffeler, M. Jean-Mairet, and E. Mugellini. Designing a Desirable Smart Bracelet for Older Adults. In *Proceedings of the 2013 ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication, UbiComp '13 Adjunct*, pages 425–434, New York, NY, USA, 2013. ACM.
- [2] G. Bieber, M. Haescher, and M. Vahl. Sensor Requirements for Activity Recognition on Smart Watches. In *Proceedings of the 6th International Conference on PErvasive Technologies Related to Assistive Environments, PETRA '13*, pages 67:1–67:6, New York, NY, USA, 2013. ACM.
- [3] G. Bieber, T. Kirsche, and B. Urban. Ambient Interaction by Smart Watches. In *Proceedings of the 5th International Conference on PErvasive Technologies Related to Assistive Environments*,

- PETRA '12, pages 39:1–39:6, New York, NY, USA, 2012. ACM.
- [4] D. Bonino, F. Corno, and L. D. Russis. dWatch: A Personal Wrist Watch for Smart Environments. *Procedia Computer Science*, 10(0):300 – 307, 2012. {ANT} 2012 and MobiWIS 2012.
- [5] L. De Russis, D. Bonino, and F. Corno. The Smart Home Controller on Your Wrist. In *Proceedings of the 2013 ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication*, UbiComp '13 Adjunct, pages 785–792, New York, NY, USA, 2013. ACM.
- [6] M. D. Dunlop, A. Komninos, and N. Durga. Towards High Quality Text Entry on Smartwatches. In *CHI '14 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '14, pages 2365–2370, New York, NY, USA, 2014. ACM.
- [7] M. Funk, A. Sahami, N. Henze, and A. Schmidt. Using a Touch-sensitive Wristband for Text Entry on Smart Watches. In *CHI '14 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '14, pages 2305–2310, New York, NY, USA, 2014. ACM.
- [8] S.-L. Hsieh, C.-C. Chen, S.-H. Wu, and T.-W. Yue. A wrist-worn fall detection system using accelerometers and gyroscopes. In *Networking, Sensing and Control (ICNSC), 2014 IEEE 11th International Conference on*, pages 518–523, April 2014.
- [9] N. Kamijoh, T. Inoue, C. M. Olsen, M. T. Raghunath, and C. Narayanaswami. Energy Trade-offs in the IBM Wristwatch Computer. In *Proceedings of the 5th IEEE International Symposium on Wearable Computers*, ISWC '01, pages 133–, Washington, DC, USA, 2001. IEEE Computer Society.
- [10] J. Knibbe, D. Martinez Plasencia, C. Bainbridge, C.-K. Chan, J. Wu, T. Cable, H. Munir, and D. Coyle. Extending Interaction for Smart Watches: Enabling Bimanual Around Device Control. In *CHI '14 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '14, pages 1891–1896, New York, NY, USA, 2014. ACM.
- [11] K. Lyons, D. Nguyen, D. Ashbrook, and S. White. Facet: A Multi-segment Wrist Worn System. In *Proceedings of the 25th Annual ACM Symposium on User Interface Software and Technology*, UIST '12, pages 123–130, New York, NY, USA, 2012. ACM.
- [12] A. Migicovsky, Z. Durumeric, J. Ringenberg, and J. A. Halderman. Outsmarting Proctors with Smartwatches: A Case Study on Wearable Computing Security.
- [13] E. Morganti, L. Angelini, A. Adami, D. Lalanne, L. Lorenzelli, and E. Mugellini. A Smart Watch with Embedded Sensors to Recognize Objects, Grasps and Forearm Gestures. *Procedia Engineering*, 41(0):1169 – 1175, 2012. International Symposium on Robotics and Intelligent Sensors 2012 (IRIS 2012).
- [14] C. Narayanaswami, N. Kamijoh, M. Raghunath, T. Inoue, T. Cipolla, J. Sanford, E. Schlig, S. Venkiteswaran, D. Guniguntala, V. Kulkarni, and K. Yamazaki. IBM's Linux Watch: The Challenge of Miniaturization. *Computer*, 35(1):33–41, Jan. 2002.
- [15] C. Narayanaswami and M. T. Raghunath. Application Design for a Smart Watch with a High Resolution Display. In *Proceedings of the 4th IEEE International Symposium on Wearable Computers*, ISWC '00, pages 7–, Washington, DC, USA, 2000. IEEE Computer Society.
- [16] J. Pasquero, S. J. Stobbe, and N. Stonehouse. A Haptic Wristwatch for Eyes-free Interactions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, pages 3257–3266, New York, NY, USA, 2011. ACM.
- [17] S. T. Perrault, E. Lecolinet, J. Eagan, and Y. Guiard. WatchIt: Simple Gestures and Eyes-free Interaction for Wristwatches and Bracelets. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '13, pages 1451–1460, New York, NY, USA, 2013. ACM.
- [18] Z. Ping. Smart Watches: Enrich People's Lives. 2013.
- [19] L. Porzi, S. Messelodi, C. M. Modena, and E. Ricci. A Smart Watch-based Gesture Recognition System for Assisting People with Visual Impairments. In *Proceedings of the 3rd ACM International Workshop on Interactive Multimedia on Mobile and Portable Devices*, IMMPD '13, pages 19–24, New York, NY, USA, 2013. ACM.
- [20] K. E. Seong, K. C. Lee, and S. J. Kang. Self M2M based wearable watch platform for collecting personal activity in real-time. In *Big Data and Smart Computing (BIGCOMP), 2014 International Conference on*, pages 286–290, Jan 2014.
- [21] M. Swan. Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0. *Journal of Sensor and Actuator Networks*, 1(3):217–253, 2012.
- [22] H. Ye, M. Malu, U. Oh, and L. Findlater. Current and Future Mobile and Wearable Device Use by People with Visual Impairments. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, pages 3123–3132, New York, NY, USA, 2014. ACM.

Copyright Notes

Permission to make digital or hard copies of all or parts of this technical report for personal use is granted without fee provided that copies are not made or distributed for profit or commercial advantage. The copyright remains with the individual authors of the manuscripts. Please consider citing the original article instead of referring to the individual contributions of this technical report.

This report has been published in the Series “*Advances in Embedded Interactive Systems*” Vol 2 (3) with the ISSN: 2198-9494