Editorial

Florian Alt* and Emanuel von Zezschwitz

Emerging Trends in Usable Security and Privacy

Abstract: New technologies are constantly becoming part of our everyday life. At the same time, designers and developers still often do not consider the implications of their design choices on security and privacy. For example, new technologies generate sensitive data, enable access to sensitive data, or can be used in malicious ways. This creates a need to fundamentally rethink the way in which we design new technologies. While some of the related opportunities and challenges have been recognized and are being addressed by the community, there is still a need for a more holistic understanding. In this editorial, we will address this by (1) providing a brief historical overview on the research field of 'Usable Security and Privacy'; (2) deriving a number of current and future trends; and (3) briefly introducing the articles that are part of this special issue and describing how they relate to the current trends and what researchers and practitioners can learn from them.

Keywords: Usable Security and Privacy, Trends

1 Introduction

The quick proliferation of our daily life with new technology in the past decade has fuelled the need to rethink the way in which we design security and privacy mechanisms. Such technology allows for *collecting sensitive data* about the user as well as to *access sensitive data* stored in the cloud. Examples include but are not limited to smart watches, smart glasses, smart home devices such as intelligent coffee machines and cleaning robots, smart speakers, and head-mounted displays.

What is striking is that the vast majority of smart devices are designed without adhering to fundamental privacy and security needs, such as encryption or authentication. This often creates a need to add security means post-hoc, for example, a smart phone app or a remote control that enables secure access to the configuration of, or data collected by, a smart home device. Such workarounds – i.e.

***Corresponding author: Florian Alt,** Bundeswehr University Munich, Research Institute CODE, Usable Security and Privacy Group
Emanuel von Zezschwitz, University of Bonn, Usable Security Methods Group

using external input and output devices – usually comes at the expense of good usability. This may ultimately lead to users trading low security for high usability, for example, not using means for security at all; or minimizing the required effort by reusing short and easy-to-remember passwords.

Beyond data collection and enabling secure information access, novel technologies also not only create *new threats* – for example, attack models based on ubiquitously available high-resolution cameras or thermal imaging [1] – but also *opportunities* – for example, novel sensor-based authentication mechanisms exploiting behavioural cues. Hence, authentication mechanisms that do not require any user action and blend with the way in which people use technology today become feasible [3].

As a result, there is a number of trends in usable security and privacy that aim to address the aforementioned challenges. In particular, the usable security community focuses on understanding the impact of novel technologies on security and privacy; identifying the needs of stakeholders in the process of designing and implementing secure interactive systems; developing novel methodologies to understand and design for emerging technologies and mitigate threats; obtaining an understanding of the nature of new application areas; and understanding how knowledge from different disciplines can be fused to built more secure, privacy-preserving, and and usable systems.

In the remainder of this editorial, we will first sketch how the research area of usable security and privacy evolved over the past decades. We will then provide a more detailed overview of trends that emerged as a result of this evolution and that are currently shifting into the focus of both researchers and practitioners. We will then conclude by briefly introducing the articles in this special issue and discuss how they relate to current trends.

2 A Brief History of Usable Security

In 1975, Saltzer and Schroeder argued that "it is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly [..]" [17]. This claim can be seen as the starting point for the research area nowadays called 'Usable Security and Privacy' [8]. Over the last decades, usable security research kept constantly growing and an impressive number of research papers was published.

User authentication has always been one of the main challenges of usable security. Therefore, we will use password research to illustrate the history of usable privacy and security. Secret alphanumeric strings, called passwords, have been

used to restrict access to specific information or services since the early days of computing. In the 1960s, the Massachusetts Institute of Technology (MIT) started using password-based user accounts on their Compatible Time-Sharing System (CTSS) [6]. At this time, asking for a password was not a usability problem since those systems were used by a few professionals for specific use cases and those users had to remember only this one secret to be entered a few times per day.

However, with the advent of the World Wide Web and the ever-increasing number of personal computers in the 1990s, alphanumeric passwords not only found their way into people's daily lives but people can access sensitive information every time and everywhere from different devices. Hence, users not only struggle with many passwords but password entry consumes a considerable part of users' time [10]. As the community understood these challenges, more academic research began to investigate the influence of user behavior on passwords and system security [2] by utilizing user-centred research approaches, known from the field of human-computer interaction (HCI).

In the 2000s, the popularity of new technologies, like smartphones and tablets as well as the growing number of cloud-based services reinforced the process and, thus, users had to manage more and more passwords. Since authentication became more important as users started storing more sensitive data in the cloud and as the web became more personalized [12], the password problem remained a hot topic in the ever-growing usable security community [11]. Starting from the 2000s, usable security and privacy research got frequently published at annual HCI-focused conferences (e.g., CHI[1]) and specialized conferences were established (e.g., SOUPS[2]).

In 2014, an average user had to manage 27 password-protected online accounts [20]. It is obvious that memorizing a unique and complex alphanumeric string for each of those accounts would significantly exceed the capacity of the human brain [7]. In recent years, the password problem became even more complex. While mobile devices nowadays often support biometric concepts for authentication, alphanumeric strings are still required as a fallback mechanism and remain the primary authentication mechanism for Internet accounts. In addition, novel device classes with various form factors became popular. For example, the popularity of personal voice-based assistants triggered research on how passwords can be used if keyboards are not available (for example, [16]). Finally, the usable security community recognized that there are different user groups which would benefit

1 Human Factors in Computing Systems Conference: https://chi2020.acm.org

2 Symposium on Usable Privacy and Security: https://soups.ece.cmu.edu/

from more usable mechanisms and started focusing on more specialized roles like administrators and software developers [15].

Today, usable security and privacy research deals with many challenges besides passwords. Such challenges involve problem areas such as social engineering (in particular, phishing), secure browsing, and online privacy. Furthermore, it focuses on different user types, cultures, environments, and device classes. The importance of usable security and privacy research is also reflected in the German research landscape. While the need to better understand how user interfaces can be built that are secure and usable at the same time has long since been understood by researchers, the past years witnessed a shift in the public perception of the topic. Politicians have understood the need to educate more experts in this area as a result of which new research centers have been founded and new study programs have been established. Usable security and privacy research and lectures are nowadays established in several universities in Germany, such as the University of Bonn, the University of Bochum, the University of Darmstadt, the Research Institute for Cyber Defense (CODE) at the Bundeswehr University Munich, or the Helmholtz Center for Information Security (CISPA) in Saarbrücken, to just name a few.

3 Current Trends

The rapid evolution of the research field on usable security and privacy has led to a number of current trends and related research questions. The way in which we as a research community address these fundamental research questions will contribute to the future design of secure and usable interfaces.

3.1 Understanding New Technologies

Technologies appear at lightning speed. The ability to easily equip novel devices with different types of sensors and networking capabilities enables novel user interfaces that provide personalized services, make users more productive, and enhance their cognitive and physical abilities. Devices come in the form of wearables (for example, smart glasses, smart watches, etc.) as well as in the form of devices placed in users' homes or work environments (for example, smart speakers).

This proliferation of our daily life with new technologies is a major challenge from a privacy and security perspective. Regarding privacy, it is often unclear, which data devices collect, where it is stored, how it is protected it, what it is used for, and with whom it is being shared. To just name one example, iRobot's

vacuum cleaning robots collect maps of people's homes, considering to sell it to third parties to provide better services[3].

Regarding security, technologies may pose unforeseen threats to users. As one example, thermal cameras, which are already integrated with many smartphones[4] or can easily be purchased as add-on to smartphones[5], allow a user's PIN or lock pattern to be easily identified as they authenticate on a smartphone [1]. Another example is virtual reality (VR) glasses. As stores, like IKEA, provide VR experiences[6], users might be asked to provide their credit card PIN while shopping in VR, being unaware of bystanders being able to shoulder surf their credentials [9].

At the same time, novel technologies also create opportunities from a security and privacy perspective. For example, they allow for creating novel means for authentication that better blend with the way in which users interact with systems. Particularly promising are so-called implicit authentication mechanisms, where no user interaction is required. One example is Skull Conduct, an authentication system for smart glasses or head-mounted devices, equipped with speakers and microphones [19]. The system analyzes characteristic frequency responses created by the user's skull to identify users. Another example is behavioral biometrics, i.e. the use of certain behavioral traits for identification, for example, typing behavior [4], touch targeting behavior [5], or gait [14].

One example of a novel authentication approach is presented in this special issue. The vein pattern identification system (VPID) uses a thermal camera to identify users from the characteristics of their veins, hence enabling authentication in application scenarios, such as on public displays or also on the smartphone.

Overall, the fact that new technologies are emerging at an ever-increasing pace creates a need for researchers in usable security and privacy to constantly explore novel technologies and understand their implication. The following questions will drive research in this area:

– How can access to a novel technology be secured?

3 iRobot to share maps of people's homes:
https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html
4 Thermal camera-equipped smartphones:
https://www.catphones.com/en-us/features/integrated-thermal-imaging/
5 Flir One:
https://www.flir.de/flirone
6 IEKA VR Experience:
https://www.ikea.com/ms/en_US/this-is-ikea/ikea-highlights/Virtual-reality/index.html

– How can the data created by a novel technology be treated in a privacy-preserving way?
– Which novel threats does an emerging technology enable?
– How can a novel technology be used to build more secure and usable interfaces?

3.2 Designing for Different Stakeholders

Traditionally, research in usable security and privacy strongly focused on the end user, in particular, on their behavior and how security mechanisms could be designed that account for this behavior. At the same time, it has been understood that designing successful security mechanisms requires considering stakeholders in all phases of product design, use, and support.

Designers. As has been mentioned before, there is a strong need to think in the design phase how appropriate means for authentication can be integrated with a product [18], most importantly means for input and output. Adding such means post-hoc is likely to result in poor usability. As a result, there is a strong need to advance our understanding how security can be made part of the design process.

Developers. Another important group of stakeholders is developers, i.e. people implementing the design of a product. Research identified that there is often a poor understanding of developers as to how basic security mechanisms can be integrated [15]. Integrating novel security mechanisms often requires effort and the benefit of this effort is not apparent. As a result, developers often focus on the primary feature which needs to be implemented and security becomes a secondary goal. For example, login and password are easy to implement but selecting the right encryption parameters is often hard for the developer.

Administrators. An often neglected group of stakeholders in research is administrators. One of the main reasons for which passwords still persist today is that they are very easy to reset. More complex and error-prone security mechanisms are often difficult to administrate and novel interfaces are required to support administrators in their work. For example, keeping systems up-to-date is a very complex task for system administrators and interaction effects are not always easy to understand [13].

Extending the scope of research in the usable security and privacy community raises a number of important and interesting questions:
– How can security and privacy be considered in the design phase of a product?
– How can developers be educated and supported to employ appropriate security mechanisms?

– How can the administration of secure and private systems be made as easy as possible?

3.3 Exploring Novel Application Areas

Security and privacy becomes increasingly important in many different contexts. In the mainframe era, authentication was limited to the workplace, the only location where users faced a need to authenticate with a computing system. Today, the fact that people can and do access sensitive information all the time and everywhere makes security and privacy protection an ever-present requirement. Examples include public and semi-public spaces, where people authenticate on their phone and payment terminals. At home, people may want to prevent couch surfers from tampering with their smart home settings. And in the car, people may want to decide whether their car insurance company gets access to their driving data in return for reduced fees.

A particular challenge arises for (personal) devices that are being used in different contexts and for access to different types of data, such as the smart phone. Depending on the context and the accessed information, a different level of security might be required. However, the current implementation – one authentication mechanism is used to protect the entire device in every situation – creates an unnecessary burden to the user. Rather, there is a need to fundamentally rethink the way in which context and for access to which information, a device is used and appropriately design authentication mechanisms.

Another challenge arises in situations, in which users are not aware of the presence of a particular technology that collects sensitive information about them. Think about somebody visiting a friend who has a smart assistant, such as Amazon Alexa or Apple Siri. Such devices may eavesdrop on conversations without people being aware of it.

As an example, one article investigates smart homes as a novel application area, focusing on users' privacy and security concerns as they consider introducing smart technologies in their homes.

This raises the following questions:

– Which information is being accessed in a particular application area and how sensitive is this information?
– How do security and privacy mechanisms that are appropriate in a particular application area look like?
– Which groups of users are present in a particular application area and how can their privacy and security needs be addressed?

3.4 Extending and Developing New Methodologies

Moving to new application areas requires an understanding of security and privacy needs in these areas. Whereas traditionally, much research has been conducted in the lab, there is an ever-increasing need to better understand the context in which technology is used and how. For example, when designing a security mechanism for smart home devices, designers need to understand how these devices are being used in order to better tailor the security mechanism to users' behavior. Understanding such behavior requires extending existing or developing entirely new approaches.

On one hand, researchers need to think about employing new *study paradigms*, such as running studies in the lab or in the field (even in the form of a long term deployment). On the other hand, there is a need to employ suitable *data collection methods*. Such methods in general strongly differ in terms of the required effort for the user and the researchers (for example, a diary study vs. automated logging of interaction) as well as the privacy implications (putting up a camera in people's homes vs. conducting a post-hoc interview).

We expect to see novel approaches in the next years that will help to, first, better understand the context for which a privacy or security mechanism is designed and that will, subsequently, help designers and developers to build appropriate mechanisms.

One example for a system that was evaluated over a longer period of time is CogniPGA, where a new graphical authentication approach was tested over several months.

We expect the following methodological questions to play a major role in the future:

- How can researchers strive a balance between obtaining fine-grained, high-quality data and preserving users' privacy?
- How can the effort both on the participant's and the researcher's side be optimized while not compromising data quality?

3.5 Learning from Other Disciplines

Traditionally, usable security and privacy is at the intersection of two major fields of research: IT security and human-computer interaction. However, the aforementioned trends make it clear that there is a strong relationship to many other fields.

For example, when designing implicit authentication mechanisms, an understanding of users' behavior is crucial. For understanding human behavior, knowledge in ethnography and behavioral economics is required. For collecting data, we believe computer vision will be a strong driver in the next years. To create models of user

behavior, there will be a strong need of expertise in machine learning. With regard to building the user interface, valuable expertise comes from the fields of warning sciences, risk perception, and persuasive technologies.

We also see a strong potential in gaming. Games have been shown as a strong means to motivate users in embracing a certain technology. As an example, one article in this special issue looks at the use of gaming in the context of 2-factor authentication.

Important research questions in this area include:
- How can the exchange of knowledge between different disciplines with regard to usable security and privacy be supported?
- How can a mutual benefit between research communities be created?
- How can a common understanding of important challenges be achieved?

4 About this Special Issue

The previous sections identified many challenges and opportunities, where they come from, and what they mean for the next decades of usable security and privacy research. The following section will briefly introduce the different articles being part of this special issue and explain how they blend with the identified trends.

The articles that are part of this special issue demonstrate, for example, how researchers can understand the current state, learn from specific contexts to improve the current state, explore novel interaction concepts, and look at visionary approaches for the next generation of security mechanisms.

4.1 Users' Privacy and Security Concerns Regarding Smart Home Technologies

This article presents a study investigating users' concerns as they think about introducing smart technologies in their homes. It presents an example of how to explore a novel application area and how this can be approached from a methodology perspective. While the stakeholders at the focus of this work are end users, it derives specific recommendations valuable for future designers and developers of such technologies.

4.2 Gamification in 2-Factor Authentication

This article explores the feasibility of providing incentives for the adoption of secure two-factor authentication (2FA) mechanisms. The authors aim to learn from the online gaming community since many games offer small rewards such as visual modifications to the player's avatar's appearance, if players utilize 2FA. Based on their lessons learned, several design approaches are presented which could help driving the adoption of secure authentication mechanisms outside of the gaming context.

4.3 CogniPGA: Longitudinal Evaluation of Picture Gesture Authentication with Cognition-based Intervention

This article presents a longitudinal evaluation of a novel authentication mechanism, called CogniPGA. The authors propose using gradually disappearing visual masks. The masks were based on eye-gaze data and applied in a way that nudges users to select a more diverse set of passwords. The results indicate that the mechanism can improve security without decreasing usability. The article illustrates how novel approaches of personalising user interfaces can help to design usable and secure authentication mechanisms.

4.4 Vein Pattern Identification

This articles introduces an approach for identifying users from their vein patterns. In particular, a thermal camera is used to record a thermal image of the user's back of the hand and different algorithms are compared regarding their recognition accuracy. This work is an example for understanding the opportunities of a novel technology and a first step towards creating novel authentication mechanisms built on top of this technology.

5 Conclusion

Usable security and privacy is a topic of ever-increasing importance in a decade in which technologies are becoming widely used in the blink of an eye. Researchers can hardly keep up with this development and a core challenge of the community

in the years to come will be to train non-experts in understanding the implications of novel technologies and design their systems and products accordingly.

In this editorial we provided a brief introduction to the history of usable security and privacy and sketched current trends that we believe will drive the research in the coming decades. We concluded by briefly introducing the articles that are part of this special issue. Those articles are primarily meant to teach and inspire readers as well as provide them some first hand examples of how current trends can be approached.

References

[1] Abdelrahman, Y., Khamis, M., Schneegass, S., and Alt, F. Stay cool! understanding thermal attacks on mobile-based user authentication. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2017), CHI '17, ACM, pp. 3751–3763.

[2] Adams, A., Sasse, M. A., and Lunt, P. Making passwords secure and usable. In *People and Computers XII*. Springer, 1997, pp. 1–19.

[3] Alzubaidi, A., and Kalita, J. Authentication of smartphone users using behavioral biometrics. *IEEE Communications Surveys Tutorials 18*, 3 (thirdquarter 2016), 1998–2026.

[4] Buschek, D., De Luca, A., and Alt, F. Improving accuracy, applicability and usability of keystroke biometrics on mobile touchscreen devices. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (New York, NY, USA, 2015), CHI '15, ACM, pp. 1393–1402.

[5] Buschek, D., De Luca, A., and Alt, F. Evaluating the influence of targets and hand postures on touch-based behavioural biometrics. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2016), CHI '16, ACM, pp. 1349–1361.

[6] Fano, R. M., and Corbató, F. J. Time-sharing on computers. *Scientific American 215*, 3 (1966), 128–143.

[7] Florêncio, D., Herley, C., and Van Oorschot, P. C. Password portfolios and the finite-effort user: Sustainably managing large numbers of accounts. In *23rd USENIX Security Symposium (USENIX Security 14)* (2014), pp. 575–590.

[8] Garfinkel, S., and Lipford, H. R. Usable security: History, themes, and challenges. *Synthesis Lectures on Information Security, Privacy, and Trust 5*, 2 (2014), 1–124.

[9] George, C., Khamis, M., von Zezschwitz, E., Burger, M., Schmidt, H., Alt, F., and Hussmann, H. Seamless and secure vr: Adapting and evaluating established authentication systems for virtual reality. NDSS.

[10] Harbach, M., von Zezschwitz, E., Fichtner, A., Luca, A. D., and Smith, M. It's a hard lock life: A field study of smartphone (un)locking behavior and risk perception. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)* (Menlo Park, CA, July 2014), USENIX Association, pp. 213–230.

[11] Herley, C., Van Oorschot, P. C., and Patrick, A. S. Passwords: If we're so smart, why are we still using them? In *International Conference on Financial Cryptography and Data Security* (2009), Springer, pp. 230–237.

[12] Kuyoro, S., Ibikunle, F., and Awodele, O. Cloud computing security issues and challenges. *International Journal of Computer Networks (IJCN) 3*, 5 (2011), 247–255.

[13] Li, F., Rogers, L., Mathur, A., Malkin, N., and Chetty, M. Keepers of the machines: examining how system administrators manage software updates. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (2019), USENIX Association, pp. 273–288.

[14] Muaaz, M., and Mayrhofer, R. Smartphone-based gait recognition: From authentication to imitation. *IEEE Transactions on Mobile Computing 16*, 11 (Nov 2017), 3209–3221.

[15] Naiakshina, A., Danilova, A., Gerlitz, E., von Zezschwitz, E., and Smith, M. "if you want, i can store the encrypted password": A password-storage field study with freelance developers. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (2019), ACM.

[16] Prange, S., von Zezschwitz, E., and Alt, F. Vision: Exploring challenges and opportunities for usable authentication in the smart home. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (2019), IEEE, pp. 154–158.

[17] Saltzer, J. H., and Schroeder, M. D. The protection of information in computer systems. *Proceedings of the IEEE 63*, 9 (1975), 1278–1308.

[18] Sasse, M. A., and Flechais, I. Usable security: Why do we need it? how do we get it? O'Reilly, 2005.

[19] Schneegass, S., Oualil, Y., and Bulling, A. Skullconduct: Biometric user identification on eyewear computers using bone conduction through the skull. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2016), CHI '16, ACM, pp. 1379–1384.

[20] Stobert, E., and Biddle, R. The password life cycle: user behaviour in managing passwords. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)* (2014), pp. 243–255.