Department: Security and Privacy
Editor: Florian Alt, florian.alt@unibw.de

Pervasive Security & Privacy – A Brief Reflection on Challenges and Opportunities

Florian Alt
Universität der Bundeswehr, München

DEVELOPMENTS IN PERVASIVE COMPUTING trigger a need to rethink security and privacy mechanisms. At the same time, security and privacy methods and systems can likewise benefit from the proliferation of pervasive computing technology, making novel approaches possible. In light of these exciting changes, beginning with this introductory column, IEEE Pervasive Computing introduces a new Security and Privacy Department in which I will invite columns on new developments and topics.

Let me first introduce myself. I am currently a full professor at the CODE Research Institute for Cyber Defense where I am head of the Usable Security and Privacy Group. With my team I look at the role of humans in security critical systems, focusing on topics related to behavioral biometrics, physiological security, social engineering, and usable security in novel application areas, such as smart homes and Mixed Reality. Prior to this I was an assistant professor in Human-Computer Interaction at LMU Munich. I received my PhD from the University of Stuttgart.

My work has for many years been inspired by Mark Weiser's vision of a world, where computing technologies weave themselves into the fabrics of everyday life [1]. At the same time, it was probably not foreseen 30 years ago how quickly this was going to happen. The speed at which technologies emerge and are about to become pervasive today is so fast that designers and developers of security and privacy approaches struggle to keep up [2]. As a result, we witness – and often even experience ourselves – an ever-increasing number of cases in which approaches to preserve privacy and protect data seem to be inappropriate as they impose considerable effort in terms of time to setup, are complex to understand, are cumbersome to use, lead to unclear consequences, and interrupt us during everyday use of computers. Think about examples, such as authentication using smart speakers, the implications of allowing a vacuum cleaning robot to share data from their camera with the manufacturer, or the need to set privacy permissions for any IoT devices that will in the future be part of smart homes.

Yet, there is hope. The ability to use sensors in personal devices and in our environment to understand contexts of use and learn about users' current behavior and states creates not just challenges but also opportunities for designing novel security and privacy mechanisms that account for

 Published by the IEEE Computer Society

the way in which users interact with technology. For example, we can infer users' context, activity, and cognitive as well as emotional state, allowing security and privacy tasks to be targeted to opportune moments.

The objective of this department is to report on current trends and developments related to security and privacy in the context of pervasive computing technology. This includes a wide variety of perspectives – from a technology point of view, but also from the view of designers, end-users, administrators, and policy makers.

This introduction is a teaser for this exciting line of research, highlighting some of the current trends and their implications, and reflecting on some challenges and opportunities – of course without claiming to be in any way complete.

THE STATE OF SECURITY AND PRIVACY IN PERVASIVE COMPUTING

Over decades, pervasive computing has constantly influenced and changed the digital assets we are protecting. In the *mainframe era*, security mechanisms were primarily implemented to protect companies' intellectual property. The proliferation of users' homes with computers in the *personal computing* era led to the need for also protecting personal assets, such as documents, images, and private conversations (email, chat). The advent of the Internet ushered in the *era of pervasive computing*, in which sensitive data could not only be accessed locally but also remotely and through an ever-increasing number of personal devices. Such technologies include smartphones, wearables (smartwatches, smart glasses), personal assistants (voice assistants, drones), smart appliances (TVs, fridges, vacuum cleaners) and smart garments, to just name a few. Beyond, there is an ever-increasing number of devices users are often not even aware of, including smart home sensors used to monitor and control heating, ventilation, air conditioning, and water consumption, implanted medical devices, electronic locks, and sensors in cars.

Almost any technology that is, or is about to become, ubiquitous raises the need for security and privacy mechanisms. From a security perspective, one driving question is how access to sensitive data can be protected. From a privacy perspective, a driving question is how users can be protected from potential consequences that result from the ability to infer sensitive information from (implicitly or explicitly) sensed data.

That these are no easy tasks and that unanticipated events create novel challenges are demonstrated by the ongoing COVID-19 pandemic: Traditionally, work and home contexts for many users were clearly separated. For example, they used different computers and phones in their offices, as opposed to in their homes. This changed suddenly as many users were forced to work from home. All of a sudden, there was not a clear distinction anymore between protecting personal assets and work assets. Laptops and phones are now commonly used both for private and business-related conversations and Internet access points at home route both personal and company traffic. This creates considerable challenges. Which novel attack routes and strategies emerge? Think about the many IoT devices inside users' private networks that, if not properly configured, allow attackers to intrude such networks. How can such attacks be mitigated? Which means for protection or which policies can be enforced by an employer at the user's home?

IMPLICATIONS

The above-mentioned example is one among many where considerable challenges emerge as a result of the many new technologies finding their way into our everyday life. I reflect on some of the implications of this development before discussing challenges and opportunities.

Security & Privacy Decision Overload

As more pervasive computing technologies are becoming part of our everyday life, the number of decisions we need to make is increasing exponentially. Think about your first personal computer, where you authenticated a few times per day to use it. With the advent of the Internet, more and more passwords were required to protect access to email accounts and online services. Today, we are required to remember many more passwords than we possibly can and the number of authentications we perform every day requires us to invest a substantial effort in terms of authentication time – in fact, research shows that the average users spends about 90

minutes per month on authentication [3].

Another example is privacy permissions, that is granting the right to devices or services to use personal data such as data on location, app usage, call logs, or contact lists. If required to do so manually for all services and devices that have or will have access to your personal data, this effort creates a considerable burden for users.

Unawareness of Data Sensitivity

Users are in many cases unaware of how sensitive the data collected about them is. Take, as an example, eye tracking data. With advances in computer vision, appearance-based gaze estimation based on the video stream from your webcam is already possible. Whereas this technology can be used as hands-free input modality, gaze data yield sensitive information on users' interests, attention, sexual orientation, to just name a few [4]. Other data that yield similar information can be obtained from a smartwatch that provides access to the user's physiological state.

There is a need to both inform the user about such implications and also to protect them – from a technical perspective as well as from a legal perspective. Attempts in the community to address such challenges were discussed at a workshop on privacy of eye tracking at the ETRA 2021 symposium[1]. A summary of both challenges and opportunities of gaze becoming a pervasive technology with regard to privacy and security can be found in Katsini et al. [5].

Sensing Close to the Body

The unawareness of data sensitivity issues is largely a result of sensing technology moving ever closer to the human body. Users are wearing smartwatches that are capable of sensing heart beat, heart rate variability and skin conductance; smart glasses include eye trackers and gyroscopes; and mixed reality headsets allow head, finger and body movements to be tracked. All the information acquired from these devices is potentially sensitive, for example, on users' health and, hence, requires protection from a privacy perspective. Yet, providers of technologies that collect and use such information currently do little to minimize consequences for users as data are leaking. Here, researchers need to look into novel ways of addressing such issues. One example is work on keystroke dynamics, where the ResearchIME keyboard filters data from private conversations in a way, such that it cannot be reconstructed later [6].

Unclear Flow of Data

The implications of security and privacy decisions become ever more difficult to grasp for users. Whereas in the pre-IoT era it was usually safe to assume that data would be kept on local devices, it is today impossible for users to understand what happens to their data as a result of granting certain privacy permissions. Which data is being collected, where is it stored, how is it processed, and who has access to it? Whereas policy makers require providing this information, the major challenge still is that such information remain rather inaccessible to users because they would be required to read long and difficult-to-understand texts about how companies treat their data. Here, novel approaches are required that allow end-users to quickly find answers to the above-mentioned questions, for example, in the form of so-called privacy labels, that provide the aforementioned information in a quick-to-perceive and easy-to-understand way[2].

Multi-Device Environments

Traditionally, access to computers and smartphones were obtained on the very device being used. Similarly, privacy settings for operating systems and browsers were made on the local computer. This has fundamentally changed. One reason is that data can, in many cases, be accessed globally. Think about a GMail account that can be accessed from a laptop, smartphone or any computer operating a browser. As a result of this expanded access, the implications of privacy settings might become unclear to users. Does revoking access to location information for the email client on one's smartphone also mean that an email provider will not use location information as emails are accessed from a laptop?

Another reason is that often there is no or no suitable input or output modalities available for performing actions related to security and

[1]PrEthics Workshop: https://prethics.perceptualui.org/

[2]Privacy Labels: https://cups.cs.cmu.edu/privacyLabel/

privacy. An example is a smart TV through which someone wants to access a video streaming platform. Entering a password using a remote control is cumbersome – so designers might decide to implement authentication using the finger print reader of the person's phone. The same strategy might be used for smart home appliances that do not come with an input device or display. This requirement for use of different input devices increases the complexity and effort for performing privacy and security related actions, potentially leading to users not understanding or not being willing to employ such mechanisms.

CHALLENGES & OPPORTUNITIES

The aforementioned implications yield many interesting questions for researchers working at the intersection of pervasive computing, security and privacy. We reflect on a few challenges and opportunities that we believe will guide emerging work in the coming years.

Designing Appropriate Mechanisms

Designers of novel pervasive computing technologies struggle with the development of appropriate security and privacy mechanisms. One challenge is that, unlike traditional user interfaces, security and privacy interfaces are only secondary to the user's main task. Hence, interface designers have to account for inattentive users who are not motivated to engage with security and privacy management and traditional user-centered design concepts are not easily applicable.

Another challenge is that with pervasive computing technologies it is often difficult to predict how people will use them (cf. the task-artifact cycle [7]). This has also implications on the design of security and privacy mechanisms. For example, a common goal is to try and minimize interruptions through prompting the user or, at least, to do this at an opportune moment – but it might be difficult to predict when such a moment is. As a result, designers often adhere to established security and privacy mechanisms that have been considered to be just good enough (e.g., authentication). It only becomes apparent later that mechanisms may not have been a particularly good choice – yet addressing issues post hoc is generally difficult. The prime example is passwords which, if used frequently and for the protection of many different assets, become cumbersome to use, due to being difficult to remember, requiring substantial time to enter, and often interrupting users during their tasks.

Hence, there is a need to think about how security and privacy can be considered during the design of pervasive technologies.

Involvement Of Different Stakeholders

It has been well understood that when it comes to designing novel security and privacy mechanisms, 'the user is not the enemy' [8]. Rather, closely involving end users is key to designing appropriate security mechanisms. At the same time, an exclusive focus on the end user is not sufficient either. Passwords demonstrate why. There are good reasons that passwords are still in use. From an end-user perspective, they represent an established concept that can be easily understood by users. They are also easy to implement – as opposed to more sophisticated mechanisms for authentication, such as behavioral biometrics, i.e., the assessment of users' behavior as a means to identify and authenticate a user. Furthermore, passwords are easy to administer because once forgotten, they can be easily reset. However, for other means of authentication, a user reset might be much more difficult to administer. Those aspects show that implementing a novel authentication mechanism with an exclusive view on one stakeholder is not sufficient, because it might create challenges for others.

Furthermore, the design of novel security and privacy mechanisms might require the involvement of new stakeholders. Think about biometrics. Here, the physiological trait or the user's behavior suddenly become the 'secret'. However, in contrast to a password, sensitive information can be inferred from the secret itself. For example, the ability to identify users from their typing or walking behavior also means that knowledge on the user's health and well-being could be derived. Hence, there is a need to think about how the user can be protected, ultimately requiring the involvement of policy makers as new stakeholders.

Out-of-the-Box Security & Privacy

The implications demonstrate that increasing complexity around security and privacy is a major challenge that users need to deal with. Many

examples show that high complexity or effort lead to users findings workarounds. As a result of the need to remember many passwords, users choose easy-to-remember passwords or reuse passwords. A common approach is to try and 'fix the user,' for example through password policies. However, this approach is not promising. Users will find other workarounds, for example, by writing down passwords on post-its. As a result, there is a need to design security procedures and systems such that they are usable out-of-the-box with as little cognitive effort and time commitment required from the user as possible.

Adaptive Security and Privacy Mechanisms

Finally, pervasive computing technologies also provide powerful means to build better security and privacy mechanisms. They allow the users' whereabouts, their current activities, their emotional and cognitive states or the people around them to be inferred. This information could be used to adapt authentication mechanisms to the current situation, to identify opportune moment in which users can be asked to engage into interaction or to take the user out of the loop.

At the same time, the use of adaptive sensing and interfaces also raises many open questions. How much control do users want to maintain? At what point do users feel patronized if decisions are taken by the system. And, is there an adverse effect by taking away security and privacy decisions from the user? If systems exert more control, users might lose the ability to behave in a secure and privacy-preserving way in situations, where there is no system making a reasonable decision for them.

CONCLUSION

Security and privacy is an important and exciting research field inside pervasive computing. As community we have not only the responsibility, but also the privilege, to be at the forefront of designing secure and privacy-preserving technologies. In upcoming issues, look for articles in this department on the exciting challenges and opportunities that lie ahead of us.

REFERENCES

1. M. Weiser, "The computer for the 21st century," *Scientific American*, vol. 265, no. 3, 1991.
2. F. Alt and E. von Zezschwitz, "Emerging Trends in Usable Security and Privacy," *Journal of Interactive Media (icom)*, vol. 18, no. 3, Dec. 2019.
3. M. Harbach, E. von Zezschwitz, A. Fichtner, A. D. Luca, and M. Smith, "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: USENIX Association, Jul. 2014, pp. 213–230. [Online]. Available: https://www.usenix.org/conference/soups2014/proceedings/presentation/harbach
4. J. Steil, I. Hagestedt, M. X. Huang, and A. Bulling, "Privacy-aware eye tracking using differential privacy," in *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications*, ser. ETRA '19. New York, NY, USA: Association for Computing Machinery, 2019. [Online]. Available: https://doi.org/10.1145/3314111.3319915
5. C. Katsini, Y. Abdrabou, G. E. Raptis, M. Khamis, and F. Alt, *The Role of Eye Gaze in Security and Privacy Applications: Survey and Future HCI Research Directions*. New York, NY, USA: Association for Computing Machinery, 2020, p. 1–21. [Online]. Available: https://doi.org/10.1145/3313831.3376840
6. D. Buschek, B. Bisinger, and F. Alt, *ResearchIME: A Mobile Keyboard Application for Studying Free Typing Behaviour in the Wild*. New York, NY, USA: Association for Computing Machinery, 2018, p. 1–14. [Online]. Available: https://doi.org/10.1145/3173574.3173829
7. J. M. Carroll, "Infinite detail and emulation in an ontologically minimized hci," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '90. New York, NY, USA: Association for Computing Machinery, 1990, p. 321–328. [Online]. Available: https://doi.org/10.1145/97243.97303
8. A. Adams and M. A. Sasse, "Users are not the enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, 1999.

Florian Alt is a Full Professor of Usable Security and Privacy at the Research Institute CODE at the Bundeswehr University in Munich. Contact him at florian.alt@unibw.de