Department: Sociotechnical Security and Privacy
Editor: Heather Richter Lipford, richter@uncc.edu; Jessica Staddon, jessica.staddon@gmail.com

Beyond Passwords – Challenges and Opportunities of Future Authentication

Florian Alt
Bundeswehr University, Munich, Germany

Stefan Schneegass
University of Duisburg-Essen, Germany

***Abstract*—Passwords have been dominating the authentication landscape for more than six decades. But while their end has been repeatedly predicted and other forms of authentication, such as fingerprint or facial recognition, have gained substantial popularity, we seem to not be getting rid of passwords anytime soon. With the proliferation of sensors in our lives – both in personal handheld and wearable devices as well as in our environments – the usable security community seems to be ready for another attempt to move beyond passwords. We shed light on current scientific developments in what is commonly referred to as *implicit authentication* – that is, authentication approaches in which physiological features and behavior authenticate users rather than explicitly engaging users in an authentication protocol. We discuss opportunities and obstacles from different stakeholders' perspectives.**

■ **THE REASONS FOR WHICH WE REQUIRE AUTHENTICATION** have substantially changed over the past decades [1]. Until the late 1980s, authentication mechanisms were primarily used as a means to protect companies' intellectual property. With the advent of the *Internet*, a need arose also in a private context to protect sensitive data that is remotely accessible, such as email conversation and, later, data used by web services and in cloud storage. The new century witnessed the arrival of *personal mobile devices* that allowed universal access to sensitive information. Finally, in the age of the *Internet of Things*, literally any device or appliance that is equipped with computing power creates a potential need for data protection, not only due to the ability to access sensitive information, but also due to their ability to collect sensitive personal information through access to sensors placed into the environment of the users or even on the users themselves.

The aforementioned developments have several implications. First, authentication happens so frequently, that the time required to do so has become a major factor, i.e. prior work showed that users spend on average more than 50 minutes per month with authentication [2]. Second, the authentication landscape has become particularly complex, with each app or service requiring different means of authentication. Third, the distinction between authentication in work and private context becomes blurred. Think about users working from home, where the choice of a weak WiFi password might make it easier for attackers to get access to company intellectual property.

This creates an inherent need to consider different stakeholders involved in the design, development, and evaluation of novel approaches to authentication, including but not limited to end users, designers, developers, and administrators. The remainder of this article sheds light on emerging requirements for future authentication before introducing implicit, biometrics-based authentication schemes as one particularly promising approach and discussing challenges for involved stakeholders.

REQUIREMENTS FOR FUTURE AUTHENTICATION

Traditionally, security and usability were considered the core characteristics of ‘good’ authentication schemes. These characteristics can be broken down into several aspects that become increasingly important. In the future, we believe that stakeholders will demand authentication systems that fulfill these requirements.

Implicitness The need for shifting to an authentication task while planning to work on a different task has long since been a major source of frustration among users. With the ability to authenticate users without their explicit involvement (similar to implicit interaction [10]), we expect one of the main weaknesses of current authentication mechanisms to vanish.

Continuity With the ability to implicitly authenticate, the question of *when* users are authenticated becomes essential. Current methods put the authentication only at the beginning of an interaction and let users use the system until their session times out or users actively log out. While this might be meaningful in a static setting, today’s computing systems require a more adaptive mode of authentication. For example, while some mechanisms protecting personal devices might be always on (e.g., while using a smartphone), it might make sense in other settings to authenticate only contextually (e.g., during particular times of the day) or depending on the current task (e.g., during using an app that exposes sensitive data).

Privacy Traditional forms of authentication, such as knowledge-based authentication or token-based authentication, do not require any privacy-sensitive information on the user be collected by the authentication mechanism. At the same time, with behavioral data becoming the basis of authentication mechanisms, there is a need to think about how the privacy of users can be protected. Consider, for example, an authentication mechanism based on gait, where the required data can be used to infer health issues, such as arthritis. Or using keystroke dynamics as a means for continuous authentication may yield information on a user’s productivity.

Ubiquity Current authentication mechanisms are designed to protect a particular device (e.g., a smartphone) or a service (e.g., access to a social network). Future authentication mechanisms are expected to work cross-device, cross-service, and cross-context. For example, as phones verify the identity of a user based on their touch or typing behavior, this knowledge could be used also by other devices such as a smart speaker or smart TV in the vicinity to authenticate the user.

FUTURE AUTHENTICATION

Novel biometric authentication schemes provide the unique opportunity to realize user authentication meeting the criteria mentioned above. In the following section we introduce three forms of implicit authentication, discuss potential application areas and discuss how they can be integrated with current approaches.

- Physiological Biometrics, i.e. the use of unique physiological features of users, are currently used for explicit authentication. Prominent examples are finger prints or face recognition on mobile phones. However, research showed examples in which physiological biometrics can also be applied in an implicit, continuous matter. For example, the Fiberio project proposes a touch screen identifying users with each press on the touch screen [5]. Using such technology, the burden of using a finger print is reduced and a continuous, implicit authentication becomes possible.

- Behavioral Biometrics, i.e. the use of unique features in human behavior to identify individuals, has recently received considerable attention in the research community. Prior work proposed their use for classical desktop setups (e.g., the use of keystroke dynamics [8]; can be used by proctoring tools) but also for ubiquitous settings (e.g., gait behavior [7]; could be used to identify people in a work context).
- Functional Biometrics combine physiological and behavioral approaches. By probing the user's body with a stimulus and recording the response, physiological user characteristics are used to identify individuals [3]. One example is the SkullConduct project that exploits bone-conduction speakers and transmission through the user's head to identify users [9].

CHALLENGES

While biometrics provide the opportunity to fulfill the proposed requirements of future authentication systems, there are still challenges to be addressed so as to foster widespread adoption. We look at such challenges from the perspective of different stakeholders who will be involved in researching, designing, implementing, using, and administrating such systems. Note that some aspects might be relevant to several perspectives.

Researcher View

The research community has invested substantial effort in better understanding behavioral biometrics authentication mechanisms. Among the investigated challenges are:

Data Sources Researchers have looked at which physiological features or behavioral traits can be the basis for future authentication [6]. Among the most popular ones are keystroke dynamics, mouse movement, and gait.

Influence on Behavior Researchers have looked at how behavior is being influenced in real settings. Influences include other users, the current context, or users' physiology [4].

Changes over Time User behavior changes over time, e.g., as a result of aging or obtaining new skills. It is yet unclear how such changes can be assessed and how often this is required.

Designer View

For decades, concepts of authentication mechanisms did not change much – rather designers usually took existing concepts and fitted them to novel classes of devices and applications. Future authentication mechanisms will create novel opportunities that designers need to deal with.

Novel Authentication Concepts Current authentication concepts employ an all-or-nothing approach. Consider a smartphone, where the authentication mechanisms requires the same action independent of whether the user plays a game, writes an email, or transfers money. Physiology or behavior-based approaches generally provide a probability of the user's identity. Novel concepts can account for this by assigning probability thresholds based on the sensitivity of the data (commonly referred to as risk-based authentication), i.e. an online banking app can require higher confidence as opposed to a newspaper app.

Opt-in/Out-out Designers need to think about how authentication mechanisms can be built in a way such that non-users are not identified against their will. Think about authentication mechanisms that infer a user's identity from their behavior using camera data. In such cases, mere passersby visible in the background should not be considered by the authentication mechanism. Authentication mechanisms might toggle between opt-out and opt-in depending on the context.

Legitimating others Traditional authentication mechanisms make it sometimes easy to provide access to third parties, i.e. handing over a token temporarily or providing others a password. The reason for this is that that there is often a high effort associated with enrollment, as a result of which users employ such workarounds. With future authentication mechanisms preventing such action, it becomes even more important to think about ways of quickly and easily legitimating others – in particular, in cases of emergency.

Application vs. Device vs. Environment We currently see two approaches to authentication: application or service-centered and device-centered. In the former approach, a device or service is protected through an authentication mechanism. Examples are web services, such as an online shopping website, or an ATM. Examples for device-centric approaches are laptops or smartphones, where access to data on the device is protected through a global mechanism. Note, that sometimes both approaches are combined, i.e. an online banking app on the smartphone implements its own authentication mechanism. For future authentication we expect an additional approach that goes beyond devices but authenticates the user in an entire environment, for example, their home. Here, input from multiple devices could be considered.

Developer View

One reason for the slow evolution of authentication mechanisms is technical complexity [1]. Due to not being considered an important part of a system, developers often employ what has been shown to be 'just good enough'. Hence, we often see passwords being employed in novel scenarios where apparently better forms of authentication that better match the way in which users interact do exist.

As a consequence, there is a need to better support the development of future authentication mechanisms. Challenges are twofold: from a software perspective, important challenges are data collection, data storage, user modeling and training, as well as re-training. From a sensing perspective, important questions are how sensors can be built or improved so as to optimally support continuous authentication and how they can be best integrated to address design challenges.

Standalone vs. Multi-factor Authentication Finally, developers need to integrate multiple biometric schemes into a single multi-factor authentication system. Multi-factor authentication can today be considered the gold standard in authentication – yet, it creates a substantial burden on the user. With implicit authentication, two approaches are possible: combining an explicit mechanism with an implicit mechanism (for example, entering a password combined with a keystroke dynamics analysis [11]) or combining multiple implicit authentication approaches.

User View

For many decades, users have been accustomed to using explicit forms of authentication. Moving authentication out of their perception is likely to substantially impact their view and behavior – similar to how the advent of the smartphone disrupted mobile computing.

Conveying Concepts Users will need to get educated about this novel authentication paradigm as no metaphors exist to help users form a mental model of respective mechanisms. This represents a huge challenge that (usable) security researchers have been faced with for decades, as they tried to introduce novel security concepts, such as digital encryption, signatures, and certificates.

Feedback With authentication sliding into the background, users will no longer have means to determine whether or not protection is active and working properly. Hence, novel ways of feedback will be required to create confidence among users.

Re-Authentication For future authentication mechanisms, user input will not be classified anymore as right or wrong – rather mechanisms will provide a probability of the user's identity, which is then compared to a threshold required by the mechanism. Re-authentication will be required either as the probability of a user being legitimate decreases or as the threshold changes (for example, as a user attempts to access an application requiring a higher threshold, cf. risk-based authentication).

Privacy Concerns Traditional knowledge-based authentication schemes are based on secrets that generally do not contain or represent personal, sensitive information. With schemes assessing human behavior this will fundamentally change, as such mechanisms, in order to work, will require personal data on the user that may

– beyond identifying the user – yield sensitive information. From this arises the challenge to build mechanisms in a way that protect users' privacy and clearly communicates this to the users. A still open question here is to which degree users need to be given control over the data collection process (e.g., when and what to collect) as well as over storage (e.g., reviewing collected data, opportunity to delete).

Data Sharing As mentioned above, authentication mechanisms need to ensure that data collected for authentication is not accessible by third parties (such as other applications), unless authorized by the user. Yet, implicit authentication schemes could benefit from data available from other applications that allow users to be identified. One example could be keystroke dynamics collected by productivity tracking mechanisms (cf. Microsoft Productivity Score). Such mechanisms are becoming increasingly popular as people agree with their employers to work from home. Here, security mechanisms can be implemented on top without further data collection, adding value for both employers and employees.

Administrators

Authentication mechanisms need to be designed, such that they can be administered with reasonable effort. This is one of the reasons behind the success of knowledge-based authentication mechanisms, i.e. secrets can be easily stored and reset. Yet, there are still many open questions which continuous authentication mechanisms pose to administrators.

Data Storage & Training One question is where the required data is stored. As such mechanisms require sensitive data, it seems reasonable to implement storage in a way such that data is kept on the devices of the end users. However, training models might require substantial computing power that is not available on devices, such as smartphones and smartwatches. In this case, data may need to be transmitted for training purposes.

Fallback Mechanisms Authentication mechanisms require a fallback, in case they fail. Common examples are users forgetting their password, losing a token, or sensors not working properly (e.g., a fingerprint sensor during rain). Biometric schemes pose a challenge, since they cannot easily be reset or changed and knowledge-based fallbacks might compromise security.

Loss of Control The use of personal devices in a working context (e.g., in home office) might lead to a loss of controls. In such contexts, should administrators be able to enforce security policies (i.e. strength of used authentication mechanism)? Another open question is how well can administrators decide which approach works best for the user and what the effect of policies on working time are (i.e. time spent to setup / use authentication).

CONCLUSION

Sensors in personal devices and our environments support another attempt to move beyond passwords – in particular, through novel implicit approaches to authentication based on different types of biometrics. We discussed how, in this way, some of the core requirements for future authentication mechanisms can be addressed. At the same time, a number of challenges lie ahead that need to be addressed by the involved stakeholders. It remains an exciting question whether implicit authentication will be able to replace passwords as the current Pareto equilibrium between usability and security [1]. Advances in artificial intelligence and computing power might render the additional costs of implicit authentication irrelevant, similar to advances in manufacturing and miniaturization enabling ubiquitous computing.

ACKNOWLEDGMENT

This project is funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – 425869382 and is part of Priority Program SPP2199 Scalable Interaction Paradigms for Pervasive Computing Environments.

■ REFERENCES

1. Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. 2015. "Passwords and the evolution of imperfect authentication." Commun. ACM 58, 7 (July 2015), 78–87. DOI:https://doi.org/10.1145/2699390

2. Ponemon Institute. 2019 “State of Password and Authentication.” Security Behaviors Report. https://pages.yubico.com/2019-password-and-authentication-report
3. J. Liebers and S. Schneegass. “Introducing Functional Biometrics: Using Body-Reflections as a Novel Class of Biometric Authentication Systems.” In Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI EA ’20). Association for Computing Machinery, New York, NY, USA, 1–7. DOI:10.1145/3334480.3383059
4. J. Liebers, M. Abdelaziz, L. Mecke, A. Saad, J. Auda, U. Gruenefeld, F. Alt, and S. Schneegass. “Understanding User Identification in Virtual Reality Through Behavioral Biometrics and the Effect of Body Normalization.” Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, Article 517, 1–11. DOI:10.1145/3411764.3445528
5. C. Holz and P. Baudisch. “Fiberio: a touchscreen that senses fingerprints.” In Proceedings of the 26th annual ACM symposium on User interface software and technology (UIST ’13). Association for Computing Machinery, New York, NY, USA, 41–50. DOI:10.1145/2501988.2502021
6. I. Stylios, S. Kokolakis, O. Thanou, and S. Chatzis. “Behavioral biometrics & continuous user authentication on mobile devices: A survey.” Information Fusion, Volume 66, 2021.
7. C. Wan, L. Wang, and V. V. Phoha. 2018. “A Survey on Gait Recognition.” ACM Comput. Surv. 51, 5, Article 89 (January 2019), 35 pages. DOI: 10.1145/3230633
8. S. Bleha, C. Slivinsky and B. Hussien, “Computer-access security systems using keystroke dynamics.” in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 12, no. 12, pp. 1217-1222, Dec. 1990, doi: 10.1109/34.62613.
9. S. Schneegass, Y. Oualil, and A. Bulling. “SkullConduct: Biometric User Identification on Eyewear Computers Using Bone Conduction Through the Skull.” Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, 1379–1384. DOI:10.1145/2858036.2858152
10. A. Schmidt. 2000. “Implicit human computer interaction through context.” Personal technologies, 4(2), 191-199.
11. Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, and Heinrich Hussmann. 2012. “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¡ (CHI ’12). Association for Computing Machinery, New York, NY, USA, 987–996. DOI:https://doi.org/10.1145/2207676.2208544

Florian Alt is a Full Professor of Usable Security and Privacy at the Research Institute CODE at the Bundeswehr University in Munich. In his research, Florian looks 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. Florian is the steering committee chair and former general chair of the MUM conference series, TPC Chair of Mensch und Computer 2020, as well as subcommittee chair of CHI 2020 and 2021. He is an editorial board member of IEEE Pervasive Computing and ACM IMWUT. Contact him at florian.alt@unibw.de

Stefan Schneegass, is an Assistant Professor of human-computer interaction at the University of Duisburg-Essen. He is interested in researching the crossroad of human-computer interaction and ubiquitous computing. Thereby, one core focus of his current research is the development of implicit authentication mechanisms. He organized several workshops at conferences such as CHI and Ubicomp. Contact him at stefan.schneegass@uni-due.de