The Authentication Dilemma

Antoni Wiercioch, Stephanie Teufel *, Bernd Teufel
University of Fribourg, international institute of management in technology (iimt), 1700 Fribourg, Switzerland.

* Corresponding author. Email: stephanie.teufel@unifr.ch
Manuscript submitted November 11, 2017; accepted May 15, 2018.
doi: 10.17706/jsw.13.5.277-286

Abstract: The design of user authentication has a significant impact on IT security or cybersecurity in general. Studies show that users put more weight on faster and more convenient access to an electronic device than on the security aspect. Classical authentication methods such as passwords are less effective because of their low practicality; around one third of users do not use passwords at all. In view of the increasing digitization and spread of smart and mobile devices, biometrics, i.e. behavior-based methods for the automatic identification of individuals, provides a user-friendly solution to the security question. In particular, behavioral biometrics as an implicit method offers a high degree of practicability with a relatively high level of security. Of course, biometric authentication cannot guarantee 100% security. Both, research and practice are facing an authentication dilemma: Increasing security is usually at the expense of user friendliness - and vice versa. The challenge is to optimize practicability and security in the authentication process.

Key words: Authentication, biometrics, cybersecurity, information security.

1. Introduction

Addressing security means protecting assets from a variety of threats. In a nutshell, information security assets primarily mean data (i.e. information), while cybersecurity assets mean far more, from individuals and businesses, to critical infrastructure, to barely tangible dimensions, such as political processes. It is about security of information networks and infrastructures, security of civil society, business and government, and thus the ability of smart structures to sustain key functions even after massive damage [1]. Here, when using the term security, we mean both information security and cybersecurity although we are well aware of the different dimension.

The foundations of cybersecurity research go back to the concept of the “CIA triangle”, which has become an industry standard. Essentially, the concept includes 3 protection goals designed to ensure information security [2]:

- Confidentiality: The confidentiality of information is guaranteed if only authorized users have access to certain information.
- Integrity: Integrity is given if the information is correct and complete and can only be changed by authorized users.
- Availability: The information must be available to an authorized user or system at appropriate time.

In order to achieve these protection goals, access rights to system users are primarily granted and administered. This process involves the identification (declaration of an identity or a user or device), the

authentication (verification of the access authorization of an identity) and the authorization (access to authenticated identities) of users [3]. As part of cybersecurity research, this three-part process is often reduced to the term "authentication". The authentication process is of high priority in security research; it is even considered by some researchers to be the most important component for ensuring overall system security [4, 5]. This is because authentication is the entry point into a system and thus acts as a preventive measure to protect a system from unauthorized access.

This paper will give an overview of authentication research with a focus on app, mobile, and smart devices and will be rounded off with an authentication modeling framework and hints for future research.

2. Explicit Authentication Methods

Traditional authentication systems rely on explicit methods that authenticate users either on the basis of their knowledge (passwords, PINs) or their ownership (chip, SIM card) [6]. The methods are called explicit because an intentional action of the user is necessary. The user must actively enter a password or insert a SIM card [5]. Although different variations of explicit methods exist in practice, the password associated with a username (identity) has remained the most widely used authentication method worldwide for around 50 years [7]. The password is a static method that grants access to a system by verifying the identity of a user once. The simple, technical implementation of this method is a major reason for the dominance of the password among the authentication methods. However, this method has numerous weaknesses that endanger the security in a system. So hackers can guess the password, for example, by repeated attempts to enter or by intercepting the password when sending it to a server [3].

Technical solutions such as data encryption are designed to prevent interception. Web page providers define minimal password length or complexity requirements so that users cannot use trivial, easy-to-guess passwords [7]. However, technical tools cannot guarantee 100% security in terms of authentication. Several studies have shown that users consciously refrain from using security measures because they rate practicability higher than security [8]-[10]. From a user's perspective, the cost of strong passwords outweighs the potential benefits or protection from potential attack [9]. For this reason, users refrain from using difficult, unique passwords as recommended by experts [11]. Ref. [12] shows that practicability is of top priority for users; the passwords of more than 6 million users who were hacked in 2011 have been analyzed: 45% of the passwords consist of numbers only. This is a big security risk because purely numerical passwords are easier to crack than alphanumeric passwords due to their low complexity. Furthermore, it has been found that 4.5% of the users use their user name as a password [12]. This indicates that users value convenience or quick access over security. Thus, humans - despite technical aids - remain a major risk factor due to their behavior; they are the weakest point in terms of security [13-15].

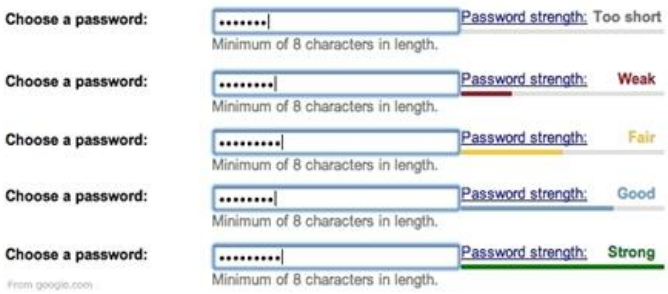

Fig. 1. Traditional password meter [17].

In order to sensitize users to the topic of password strength, password meters are increasingly used on websites [7]. The user is shown how strong the entered password is (Fig. 1). Password strength is calculated due to the complexity of the password. The website operators intend that users choose stronger

passwords, e.g. consisting of at least eight characters, small, capital letters, and special characters. However, studies showed that password meters displaying password strength are not always effective. Ref. [16] found that password meters are effective only on accounts that users find important and critical to their security. Traditional password meters are therefore not very useful because the effectiveness depends on the context or the subjective perception of a user regarding the importance of a particular application.

Some researchers attribute the ineffectiveness of security measures to users' lack of IT knowledge [18], [19]. Thus, password meters are ineffective because users lack the ability to interpret password strength due to absence of expertise. As a result, users can not judge the impact of a weak, medium or strong password on security [18]. Ref. [18] shows that additional information about password strength significantly influences user behavior. For example, users choose significantly stronger passwords if the password meter provides additional information, such as how long it takes a hacker to crack the password. The strongest positive effect is achieved if the entered password appears in a strength ranking with other users. The findings of [18] show that the effectiveness of password meters can be significantly increased by adding less information as the basis for interpretation. This approach is easy to implement and cost effective.

Another reason for poor passwords can be attributed to increasing digitization. On average, users have 16 online identities (login & password). This is about one third more identities than in 2009 [3]. The increases in online identities in connection with the increasing password requirements on the part of website operators cause users to reuse certain passwords. In addition, certain applications require users to periodically renew their passwords [19]. In order to face these challenges, users often resort to three practices [11]:

a) Write down passwords: This carries the risk that the password list will be accessible to other persons.
b) Multiple use of a password on different websites (possibly slight modification): Cracking the password of an identity automatically gives access to all other identities of this user.
c) Password managers: Users need to remember just one master password and can so manage other passwords. Cracking the master password automatically gives access to all identities of that user.

Despite the high level of user acceptance and the simple technical implementation, passwords are burdened with many weaknesses. Password meters and minimum requirements for the password compilation on the part of website providers are only partial solutions and cannot fully guarantee the system security, since many users do not use strong passwords for convenience reasons. Object-based (token) or proprietary authentication methods (chip, license key) also have weaknesses because they might be stolen or lost [4]. In addition, ownership-based methods actually authenticate only the tokens, rather than a specific person. These methods merely assume that the verified token belongs to the legitimate user [10]. Even if knowledge and ownership (password and token) are combined into a multi-factor authentication, no much better results can be expected.

3. Biometrics

3.1. Physiological Biometrics

In addition to knowledge and ownership-based authentication methods, it is possible to authenticate users through physiological biometrics. Here, an individual is identified via personal body features such as iris, retina, fingerprint or facial features. To grant a user access, the system compares the biometric properties with a master template or previously collected user biometric data [5]. The main difference to classical methods is that matching is based on available biometric data, which are compared with a master template to calculate a matching score. If this value exceeds the allowed limit, the user is identified and authenticated as a legitimate user. One speaks in this context of a 1:N comparison, since the system

compares the template to be verified with all other templates in a database [6]. It should be noted, that a 100% match score is almost impossible because biometric features may change (e.g. retinal damage, work accidents on hands) or be distorted by environmental conditions, such as different lighting conditions or camera angles [3]. Thus, a 100% match might be seen as fraud. For reasons of practicability, the limit should be set in an interval below 100%. In contrast, classical methods use 1:1 matching; since the credentials to be verified (e.g. user name and password) must be 100% identical to the previously collected data by a user to verify and to authenticate [5].

Biometric authentication provides some advantages over classical methods. For example, a user can have multiple identities using biometric data without having to remember a single password or having tokens available [3]. The user always carries the access data in the form of his biometric features. The high practicability is an important strength of this method.

Despite the high practicability, biometric authentication is burdened with weaknesses that are not negligible in the security context. The disadvantages lie in the nature of the screening and matching process. Since a perfect match is difficult to achieve, authentication is not always possible. This results in two types of errors: False Rejection Rate (FRR) and False Acceptance Rate (FAR). FRR denies access, even though the user would be legitimized. The frequency of this type of error increases the higher the threshold value of the match is set. FAR arises when an unauthorized user is mistakenly authenticated. While the FRR reduces usability, the FAR poses a security risk. From a technical perspective, the difficulty is to optimize the matching thresholds to balance practicability and security. Other weaknesses stated by [3] include the unresolved privacy issues related to biometrics and the high cost of hardware components such as fingerprint scanners. These disadvantages are the main reasons why physiological biometrics has not reached the masses of users and traditional application providers' authentication methods are favored [3].

3.2. Mobile Authentication

The continuing superiority of classical authentication methods is due, among other things, to the widespread use of PCs and laptops. The fixed-in-place devices increase the effectiveness of methods such as tokens, biometric scanners or passwords. However, the use of mobile devices (tablets, smartphones, wearables) questions the classical methods. Since 2012, PC manufacturers have seen a decline in sales, while the demand for smartphones continues to rise. This demand shift has an impact on the effectiveness of authentication methods. Classical methods are mainly aimed at stationary devices. Mobile devices are often used in public places, why they are more vulnerable to theft or shoulder-surfing (spying) than PCs and laptops. As a result, classical authentication methods on smartphones are less effective because, for example, strangers can spy on a user's login information in public places.

Furthermore, the handling behavior of smartphones has an impact on the acceptance and thus effectiveness of explicit authentication methods. In contrast to the PC, more interruptions occur when using a smartphone, which means that the user is often asked to authenticate. On average, users activate their smartphone 83 times a day and unlock it 47 times. Activation refers to checking time and messages, while unlocking requires entry of a PIN or similar [20]. It can be assumed that users interact several hundred times per day with their smartphone. For quick device access, users typically use simple, easy-to-remember PINs, patterns, or passwords for authentication. Around one-third of users even completely opt-out of smartphone authentication [21,10]. The security risk is obvious when users automatically save the passwords for other identities in the web browser and their smartphones are stolen. Thieves have virtually unlimited access to all applications in this case.

3.3. Behavioral Biometrics

Alternative authentication solutions, such as biometric techniques, are required because classical

methods are less effective in the mobile context. In addition to physiological biometrics, behavioral biometric data are increasingly used. Behavioral biometric authentication is based on a user's behavior [6]. Smartphones play an important role in the implementation of this approach, since they can be understood as the measuring device: a variety of sensors such as accelerometer, gyroscope, magnetometer, camera, and thermometer are employed to measure behavioral data (Fig. 2). For example, data about certain movements, gait recognition, keystroke and key press or the online behavior of a user are collected and evaluated. If the data matches the master template, the user is authenticated [21].

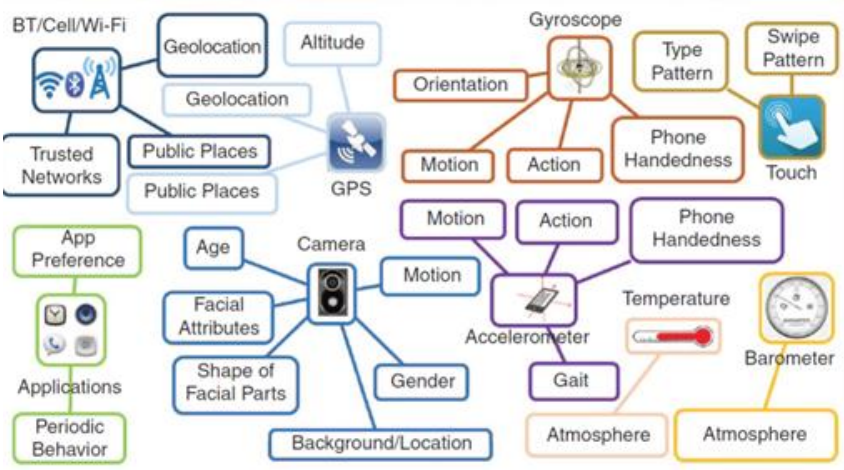

Fig. 2. Mobile device sensors for implicit authentication [21].

The strength of behavioral biometrics lies in the implicit capture of user data. This means that the user does not have to actively take a security measure (e.g. PIN input), but the system checks and analyses the behavior of the user in the background [22]. In this context, we speak of dynamic or continuous authentication because user behavior is checked while the device or application is being used. Once the system detects an anomaly, the user is denied access and is asked to confirm his identity using an alternative method, e.g. PIN or password [21].

Geospatial data can also be used as an implicit method of user verification. For example, app access may be denied if it is from an unusual location (e.g., from abroad). The user would then have to answer additional personal security questions to log in.

In literature, the benefit of implicit authentication is seen to be highly practical and secure [23]. Practicality is ensured by the fact that the smartphone can be used freely, without having to think about authentication. The continuity of authentication increases security: In contrast to explicit authentication, the implicit method ensures that the user is the legitimate user even after logging in, i.e. while using a device. Explicit methods, on the other hand, only validate the identity during the login process, not during use [23]. Ref. [10] shows that 92% of users perceive implicit authentication as more secure than traditional methods.

A weakness of continuous authentication lies in the demanding computing power. The processing power and limited storage capacity on mobile devices have an impact on the acceptance of the method, because the permanent authentication slows down the system. The latency (delays) caused by the calculations is a practicality deficit because it limits the operation of a mobile device [10]. As a result, long latencies adversely affect the acceptance of continuous authentication. Ref. [23] also mentions that the battery life of the smartphone is shortened by continuous authentication. Therefore, it is important to use energy-efficient authentication modules to ensure user-friendliness.

In addition to local authentication (on the smartphone), it can also be done via a server or a cloud [24].

The network-based method is particularly used for complex software that processes particularly large amounts of data [25]. Server-based authentication requires Internet connection and poses a greater security risk since it is more vulnerable than local authentication [24]. The biggest risk is that the biometric data, both physiological and behavioral, are revealed. In this case, the data would be forever compromised because biometric data is unique and cannot be changed [26].

The biggest problem of implicit authentication - for both physiological and behavioral biometrics - remains the error rates, especially the FAR. Numerous studies investigate the accuracy of behavioral biometric identifiers (classifiers). Classifiers are, for example, the keystroke, GPS data, the walking pattern or the arm movements. The accuracy of the authentication systems differs greatly and depends on the test conditions and the selected classifiers. In different studies, the accuracy varies from 50% [27] to more than 90% [25]. It turns out that physiological features authenticate more reliably than behavioral biometrics. In addition, multimodal systems that use multiple classifiers are more accurate than systems that rely on single methods, such as keystroke only [21]. However, [25] mentions that an increase in classifiers does not necessarily provide the best results, but the combination of very specific sensors.

While most research addresses "how?" (explicit vs. implicit) and "when?" (one-time vs. continuous) of authentication, the question of "where?" is hardly addressed. The vast majority of the work relates to a device-based authentication, which means that it is checked in principle whether a user may use a specific device. Ref. [28] shows that 12% of the users share their smartphone and 27% share their tablet. This complicates implicit authentication, because a unique biometric profile cannot be created when a device is used by different users. The case of multiple users is particularly important in multi-person households. So it is conceivable that notebooks, tablets or other smart devices are shared in the household. Therefore, instead of device-based, application-based (app-specific) authentication is required [29]. The idea is that application-centric authentication uses those classifiers that are most accurate for a specific application. For example, a chat app would tend to use keystrokes as the dominant authentication method while the web browser authenticates based on online behavior (visited web pages). The choice of classifier would be outsourced to the app developer who creates the logic of the authentication system. Accordingly, the app decides how and when the user is authenticated [29]. Ref. [29] shows that the error rate (FAR) can be reduced to one-half or even one-third when the classifiers are adapted to specific applications.

App-specific authentication also mitigates the security risk of disclosing biometric data, since in an attack "only" the app-specific biometric data are affected. It should be noted that according to [28] users want to use around half of their apps without authentication. This can be enabled by app-specific authentication, as smartphones limit access to one-time authentication (such as PIN) by default. If the user authenticates, he can use the smartphone with all functions. If the user cannot authenticate, access is completely denied. Ref. [28] argues that this all-or-nothing policy neglects the needs of users. Depending on the app type, users want different access permissions. Thus, three categories of access permissions are possible [28]:

- Apps that always require authentication (e.g. financial app).
- Apps that require authentication for individual features (e.g. shopping app).
- Apps that do not require authentication or are always freely accessible (e.g. music app).

The findings of [28] suggest that an individualized al-location of authentication methods is preferred rather than an all-or-nothing attitude; 75% of users prefer implicit authentication. The app-specific authentication would so increase practicability and security, as the consideration of the individual authentication preferences optimizes the user-friendliness and security for the individual user. For device-based authentication, there is a risk that users will completely relinquish authentication for convenience.

4. Authentication Framework and Future Research

A looming weakness in authentication research is evident in the methodology of the studies. Often, new authentication methods are performed under laboratory conditions with very small samples. The sample size is often 20-30 test persons (cf. [24, 25, 29]), but larger samples are needed to ensure the generalizability of the results. In addition, to be criticized are laboratory conditions whereby test takers test only certain applications and fulfill predefined tasks. This limits the scope for action. Whether an authentication method actually applies and is effective in terms of security is only apparent in the real environment.

The authentication modeling framework shown in Fig. 3 provides an overview of how authentication can be designed. All methods have advantages and disadvantages, which is why emerging, implicit methods alone cannot really increase security. Rather, it is about the pooling of different methods to ensure the highest possible level of security. It turns out that the practicability of an authentication method belongs to the highest priority of the users and thus security depends on the user acceptance. Users who do not accept a specific authentication will bypass the security barriers, for example through easy to remember but at the same time easy to guess PINs or passwords.

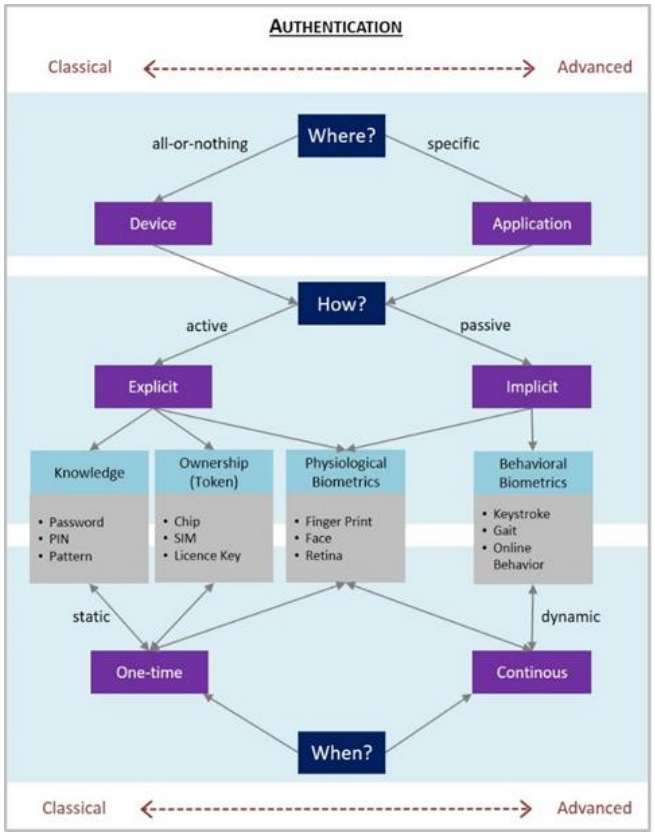

Fig. 3. Authentication modeling framework according to [5].

Both research and practice should accept that absolute security is difficult or impossible to achieve. As long as users have the ability to bypass authentication mechanisms for convenience, there will be a security risk to any system. Consequently, future research should look at how to best balance practicability and security. One approach is to study user acceptance and user preferences for authentication methods. It is assumed that the individual configuration of the authentication maximizes the practicability for each user and thus ensures the maximum security for each user. To answer the question of how authentication should be individualized, the framework in Fig. 3 can be used.

5. Conclusion

The choice of authentication method has a significant impact on security. The difficulty is to choose an authentication method that optimally balances practicability and security. This aspect is all the more important as different studies show that users weight faster access to a device higher than security. Recent research indicates that implicit authentication methods, which mostly authenticate users by means of behavioral biometrics, can increase both security and practicability. Compared to explicit methods, such as passwords or PINs, implicit methods are more user-friendly because the authentication runs in the background, without any active user interaction. The high practicability of the implicit method is of great importance because users often forego explicit authentication methods for convenience. The deactivation of security measures deprives the explicit methods of effectiveness. Against this background, the question arises whether the implicit methods with an accuracy of 90-99% may not provide more security than deactivated explicit security measures.

Acknowledgment

The authors wish to thank the members of the iimt Crowd Energy team as well as the smartlivinglab team for fruitful discussions. This work was supported by the Canton of Fribourg, Switzerland, through the smartlivinglab project at the University of Fribourg.

References

[1] Teufel, S., & Teufel, B. (2015). Smart Living – An Innovation and Research Agenda. *Proceedings of the 2015 World Conference on Innovation, Engineering, and Technology*, Kyoto, Japan.

[2] Whitman, M. & Mattord, H. (2016). *Principles of Information Security* (6th ed..). Boston: Cengage Learning.

[3] Laurent, M. & Bouzefrane, S. (2015). *Digital Identity Management*. London: ISTE Press - Elsevier.

[4] Ashibani, Y., Kauling, D. & Mahmoud, Q. (2017). A context-aware authentication framework for smart homes. *Proceedings of the IEEE 30th Canadian Conf. on Electrical and Computer Engineering*.

[5] Amin, R., Gaber, T., ElTaweel, G. & Hassanien, A. (2014). Biometric and traditional mobile authentication techniques: Overviews and open issues. In Hassanien, A. et al. (Eds.), *Bio-inspiring Cyber Security and Cloud Services: Trends and Innovations*. Heidelberg: Springer.

[6] Matayas, V. & Riha, Z. (2003). Toward Reliable User Authentication through Biometrics. *IEEE Security & Privacy*, 99(3), 45-49.

[7] Furnell, S. (2011). Assessing password guidance and enforcement on leading websites. *Computer Fraud & Security*, *12*, 10-18.

[8] De, L., Hang, A. A., Zezschwitz, V. E., & Hussmann, H. (2015). I feel like I'm taking selfies all day! Towards understanding biometric authentication on smartphones. *Proceedings of the 33rd Ann. ACM Conf. on Human Factors in Computing Systems* (pp. 1411-1414).

[9] Herley, C. (2009). So long, and no thanks for the externalities: The rational rejection of security advice by users. *Proceedings of the ACM New Security Paradigms Workshop* (pp. 133-144).

[10] Clarke, N., Karatzouni, S. & Furnell, S. (2009). Flexible and transparent user authentication for mobile devices. In Gritzalis, D. & Lopez, J. (Eds.), *Emerging Challenges for Security, Privacy and Trust. SEC 2009. IFIP Advances in Information and Communication Technology*.

[11] Ion, I., Reeder, R., & Consolvo, S. (2015). «...No one can hack my mind»: Comparing expert and non-expert security practices. *Proceedings of the Symp. on Usable Privacy and Security (SOUPS)* (pp. 327-346).

[12] Shen, C., Yu, T., Xu, H., Yang, G. & Guan, X. (2016). User practice in password security: An empirical study

of real-life passwords in the wild. *Computers & Security*, *61*, 130-141.

[13] Teufel, S., & Teufel, B. (2015). Crowd Energy Information Security Culture: Security Guidelines for Smart Environments. In *Proc. IEEE Smart Cities 2015*, (pp. 123-128).

[14] Schlienger, T., & Teufel, S. (2002). Information security culture: The socio-cultural dimension in information security management. *Proceedings of the IFIP TC11 17th Int. Conf. on Information Security: Visions and Perspectives*.

[15] Da, V. A., & Eloff, J. (2010). A framework and assessment instrument for information security culture. *Computers and Security*, *29(2)*, 196–207.

[16] Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K., & Herley, C. (2013). Does my password go up to eleven? The impact of password meters on password selection. *Proceedings of the CHI*.

[17] Ui-Patterns. (2017). Password strength meter design pattern. Retrieved October 19, 2017, from http://ui-patterns.com/patterns/PasswordStrengthMeter

[18] Khern-am-nuai, W., Hashim, M., Pinsonneault, A., Yang, W., & Li, N. (2017). Designing better password strength meters by incorporating contextual information. Retrieved October 19, 2017, from https://ssrn.com/abstract=2800499

[19] Adams, A., & Sasse, M. (1999). Users are not the enemy — Why users compromise computer security mechanisms and how to take remedial measures. *Communications of the ACM*, *12*, 40-46.

[20] Harbach, M., Von, Z. E., Fichtner, A., De, L. A., & Smith, M. (2014). It's a hard lock life: A field study of smartphone (Un)locking behavior and risk perception. *Proceedings of the Symp. on Usable Privacy and Security (SOUPS)* (pp. 213-230).

[21] Patel, V., Chellappa, R., Chandra, D., & Barbello, B. (2016). Continuous user authentication on mobile devices. *IEEE Signal Processing Magazine*, *33(4)*, 49-61.

[22] Yang, Y., Sun, J., & Guo, L. (2016). PersonalA: A lightweight implicit authentication system based on customized user behavior selection. *IEEE Trans. on Dependable and Secure Computing*, *99*.

[23] Yohan, A., Lo, N., & Lie, H. (2016). Dynamic multi-factor authentication for smartphone. *Proceedings of the IEEE 27th Int. Symp. on Personal, Indoor and Mobile Radio Communications*.

[24] Alghamdi, S., & Elrafaei, L. (2017). Dynamic authentication of smartphone users based on touchscreen gestures. *Arabian Journal for Science and Engineering*, *7*, 1-22.

[25] Lee, W., Liu, X., Shen, Y., Jin, H., & Lee, R. (2017). Secure pick up: Implicit authentication when you start using the smartphone. *Proceedings of the SACMAT'17* (pp. 67-78).

[26] Patel, V., Ratha, H., & Chellappa, R. (2015). Cancelable biometrics: A review. *IEEE Signal Processing Magazine*, *32(5)*, 54-65.

[27] De Luca, A., Hang, A., Brudi, F., Lindner, C., & Hussmann, H. (2012). Touch me once and i know it's you!: implicit authentication based on touch screen patterns. *Proceedings of the SIGCHI Conf. on Human Factors in Computing Systems (CHI'12)*(pp. 987-996).

[28] Hayashi, E., Riva, O., Strauss, K., Brush, A., & Schechter, S. (2012). Goldilocks and the two mobile devices: Going beyond all-or-nothing access to a device's applications. *Proceedings of the 8th Symposium on Usable Privacy and Security*.

[29] Khan, H., & Hengartner, U. (2014). Towards application-centric implicit authentication on smartphones. *Proceedings of the 15th Workshop on Mobile Computing Systems and Applications*.

Antoni Wiercioch holds a master's degree in business administration. His fields of interest are entrepreneurship and digital business. He worked as a junior researcher at the international institute for management in technology (iimt), University of Fribourg,

Fribourg, Switzerland. His research addresses cybersecurity issues with a focus on behavioral aspects and authentication methods.

Stephanie Teufel studied informatics at the Technical University of Berlin and the Swiss Federal Institute of Technology Zurich (ETH Zurich). She received her Doctor's degree from the University of Zurich in 1991. She was a lecturer at the University of Wollongong, Australia, and a university professor in information systems at the Carl von Ossietzky Universität Oldenburg, Germany. Since 2000 she holds a full professorship in management in information and communication technology at the Faculty of Economics and Social Sciences, University of Fribourg, Switzerland. Furthermore, she is the Director of the International Institute of Management in Technology (iimt). Her research interests include cybersecurity management, smart living and energy systems management, innovation and technology management.

Bernd Teufel studied computer science at the University of Karlsruhe, Karlsruhe, Germany. Subsequently, he joined the Department of Computer Science, ETH Zurich, where he received his doctor's degree in 1989. He was a lecturer at the Department of Computer Science, University of Wollongong, Australia, and a scientific consultant with Commonwealth Scientific and Industrial Research Organization (CSIRO), Sydney, before he founded an IT company in Germany. After several mergers, he left the organization in 2008 and founded a consultancy agency in Switzerland in 2009, mainly focusing on independent research mentoring. His research interests include ICT & cybersecurity management, management of energy systems, and innovative smart living approaches.