Authentication in a Hyperconnected World: Challenges, Opportunities and Approaches

Christoph Lipps[1], Jan Herbst[1], Rekha Reddy[1], Matthias Rüb[1], and Hans Dieter Schotten[1,2]
[1]German Research Center for Artificial Intelligence (DFKI), Germany
[2]University of Kaiserslautern (RPTU), Germany

Christoph.Lipps@dfki.de
Jan.Herbst@dfki.de
Rekha.Reddy@dfki.de
Matthias.Rueb@dfki.de
Hans_Dieter.Schotten@dfki.de

Abstract: Authentication and integrity are the prerequisites for trustworthy and secure communication. Without unambiguous knowledge of who is being interacted with, no confidential content can be exchanged, no (remote) access to systems and equipment can be granted, and no trust can be established. This situation is further exacerbated by an increasing interconnection and globalization towards a hyperconnected world. (Communication) Participants are no longer necessarily in close physical and social proximity and do not need to know each other, but can have their source/destination anywhere in the world. An authentication process is used to verify that someone -whether human or machine-, is in fact who she claims to be: The process thus includes a validation step to evaluate an assertion. However, systems differ in terms of their requirements, for instance with regard to the authentication options available, the time period required for re-authentication and the frequency of re-authentication, as well as the level of security to be achieved with authentication. The latter particularly with regard to the cost/benefit ratio of the application. Additionally, there are efforts to finally abolish traditional passwords, passphrases and pin codes and render them obsolete. In this work, technologies and methods for authentication beyond passwords and trustworthy authentication will be examined, particularly with regard to future communication infrastructures such as Beyond 5G and Sixth Generation (6G) wireless systems. Thereby, the impact of Artificial Intelligence (AI) methods, but also the relevance to Quantum Key Distribution (QKD) and Post Quantum Cryptography, as well as the use of 6G-enabling technologies like Reconfigurable Intelligent Surfaces (RISs), Wireless Optical Communication (WOC) and Physical Layer Security (PhySec), for example as additional factors of a multi-factor authentication process, will be considered, along with Body Area Networks (BANs) and the integration of the human body relying on biometrics. The various concepts are compared with regard to their requirements, limitations and possible applications in order to provide the user with an orientation as to which authentication method is conceivable and useful in which specific scenarios.

Keywords: Beyond 5G, 6G, Physical layer security, Physically unclonable functions, Human-PUFs, Channel-PUFs, (Cyber)Security, Sixth generation

1. The Hyperconnected World: A Vision for the Future

The future will be inter- and hyperconnected: According to the Cisco Annual Internet Report, 2018 there were around 480 million interconnected devices, by 2023 there are 823 million, however, it is expected that by 2030 there will be more than 50 billion interconnected devices with a data volume transmitted of up to 350 to 400 zetabytes (Cisco, 2020). Communication systems will thereby be the core element of digital value creation and society, as well as the technological foundation for digitalisation and thus the enabler of innovation and progress. Particularly in sectors such as the (Industrial) Internet of Things (I)IoT, right the way through to an industrial metaverse in which machines, factories, buildings, cities, networks and transport systems are virtually mirrored and digitally twinned (DT), via applications such as Augmented and Extender reality (AR/XR), and autonomous driving, big data analytics and global connectivity will be commonplace. As highlighted in **Figure 1**, a number of additional factors contribute to the hyperconnectivity scenario. These include the integration of low orbit satellite communication, drones and space exploration technologies, as well as aspects of sustainability. In this all-electric society with smart cities and connected healthcare system - up to a medical metaverse -, the confidentiality, reliability and resilience of networks and systems are essential. Artificial Intelligence (AI) methods will be integrated at every level of the processing chain, in central nodes and cloud environments, to calculate and train complex systems, but also in the fog and at the edge (Kimovski, et al., 2021). This requires an appropriate infrastructure in terms of bandwidth, latency and throughput on the one side, and on the other side there are demands on the reliability of the AI in terms of Trusted AI and Trustworthy AI (Ma, et al., 2023).

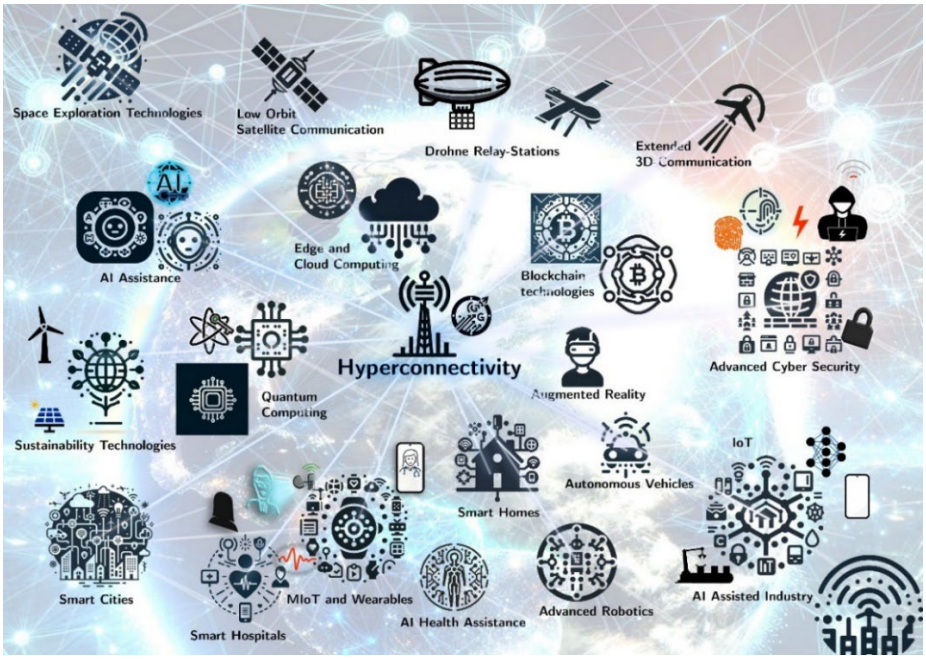

Figure 1: Hyperconnectivity in the future: efficient, sustainable and secure hyperconnectivity as an enabler of an all-connected world[1]

Although the quest for security and trust is perhaps as old as humanity itself -potential threats posed by strangers have always had to be recognised, mitigated and at best prevented-, trust must be developed, maintained, and reinforced (Lipps, et al., 2023). But with increasing globalisation and interconnection, combined with the ability to remotely access systems -it is no longer necessary to be in close proximity to access a system-, and with the rising importance of transmitted data in terms of confidentiality and privacy, the motivation for hackers and saboteurs is rising as well. For instance, the attacks to Cyber-Physical critical infrastructure, such as to water systems (Tuptuk, et al., 2021), the Colonial Oil Pipeline (Lipps, et al., 2022) and the KillNet Distributed Denial of Service (DDoS) attack to the health and energy sector (Tolanur & Chaudhari, 2023) are evolving and are every day threats (Ciocarlie & Zhou, 2023). Furthermore, there will be a series of AI-based attacks in the future. These include, among others, attacks with the assistance of AI, as it is already happening today with deepfakes (Chadha, et al., 2021), for example; but also attacks on AI, such as ii) the conscious manipulation of data by data poisoning (Tolpegin, et al., 2020) or backdoor attacks on AI models (Lin, et al., 2020).

The hyperconnected world of tomorrow is promising many simplifications, improvements and new capabilities, but its realisation will significantly depend on the success of a series of enablers:

- Powerful, efficient and sustainable telecommunication infrastructure => Beyond 5G and 6G technology
- Artificial Intelligence and their applications => Distributed AI, Trusted AI and Trustworthy AI
- Cyber-Resilience and Cyber Security => Security, Privacy and Resilience of infrastructure and applications

To elaborate on this, the rest of the work is structured as follows: A definition of the concepts of "identification" and "authentication", as well as a categorisation and the current status, are given in Section 2. Furthermore, Section 3 addresses the challenges arising and proposes technological possibilities for future methods. These are discussed in Section 4 and an overview of the strengths and weaknesses is given, followed by Section 5, which concludes the work and provides an outlook for future work.

2. Identification and Authentication: The Status Quo

In a hyper-networked world, as in the field of information security and social relations in general, the functions of identification and authentication are of fundamental importance and are strictly related. Whereas

[1] Please note: This image was generated with the assistance of AI

identification is the process by which an entity claims its identity, authentication is the proof, the validation of this claim. These concepts are emphasised in more detail and brought together for secure communication in the future.

2.1 Understanding Identification and Authentication

Especially because (biometric) identification is as old as humanity itself (see Biometrics) and there is a multitude of more or less sophisticated methods for validation available over time, a basic definition and objective understanding of the term is necessary. Therefore, the National Institute of Standards and Technology (NIST) describes authentication as “a process of establishing confidence” (Burr, et al., 2013). In combination with *Burrows, Abadi & Needham* which are specifying it in detail with the technical perspective, that "after authentication, two principals should be entitled to believe that they are communicating with each other and not with intruders" *(1990)* and together with *O’Gorman*’s requirements about a “process of positively verifying the identity” *(2003)* of an entity, an adequate indication can be made: *establishing confidence* and *verifying the identity* form the very fundamentals of a trustworthy communication whereupon secure exchange of information can be built on.

Already with the emerging idea of distributed systems and the growth of network technology in the 1990s, *Burrow, Abadi & Needham* demanded that "authentication protocols are the basis of security in many distributed systems" *(1990)*. This is emphasised by *Bruce Schneier* in relation to access control, which cannot be carried out until the identification -"who are you"-, and authentication -"and can you prove it"-, have been completed (Schneier, 2000). Historically, several protocols have decisively influenced the modern understanding of authentication. These include the Needham-Schröder protocol (Needham & Schroeder, 1978), Otway-Rees (Otway & Rees, 1987) and Kerberos (Garman, 20023), each contributing to the development of secure authentication mechanisms in various systems. Thereby, the practical aspect of authentication involves a dual responsibility, granting access to legitimate users, while at the same time denying and limiting it to unauthorized entities.

Furthermore, *Schneier* insightfully links the concepts of security and trust, by highlighting that “security is what you need when you don’t have any trust” and “security is ultimately […] (to) introduce trust in society” (Schneier, 2012). However, at the same time, he also emphasises the holistic approach to authentication and security as “cryptography is not a panacea – you need a lot more that cryptography to have security – but it is essential” (Schneier, 2000). The factors influencing the effectiveness of identification and authentication process include the availability of information, the type of the system and use-case, the access level and the potential use of cryptographic keys.

2.2 Multi-Faktor Authentication: Principle and Factors

In the heterogeneous landscape of information security, the development of authentication methods has been driven primarily by the balance between robust security and user-friendly access. Over decades, passwords, for instance, have been the cornerstone of secure systems. Their simplicity and ease of implementation made them ubiquitous in almost every application. However, passwords also have significant weaknesses, as Bruce Schneier emphasizes: For convenience, users often choose a password to easy to guess, whereas if they are forced to generate a complex one, they write it on a post-it (Schneier, 2000). The habit of using the same password for multiple platforms, as well as the willingness to share a password with others, especially when it is helping to get work done, exacerbates this vulnerability (Schneier, 2000).

Given these limitations, there are efforts in academia to replace text passwords. In their comprehensive study *Bonneau, et al.* (2012) describe these efforts and discuss different approaches, such as graphical and cognitive methods, which they contrast in detail. In addition, there have been approaches for many years, for example to use existing social media accounts (social login) (Ho & Katuk, 2016) or to be able to access multiple applications with a single set of credentials (single sign-on (SSO)) (Radha & Reddy, 2012).

If a single factor, such as a password, is used, this is referred to as Single-Factor Authentication (SFA). Adding another factor to the system is called 2-Factor Authentication (2FA), while 3-Factor Authentication is called Multi-Faktor Authentication (MFA) and 4-Factor Authentication or more is known as Strong Authentication (SA) (Schneier, 2015). Typically, MFA is designed to use factors from different areas: i) something you know (such as passwords); ii) something you have (cards or tokens); iii) something you are (biometrics). There are also current efforts to include context as an additional factor in the process to increase plausibility and security (Huseynov & Seigneur, 2017).

Nevertheless, on the path to replacing conventional mechanisms, it will play a decisive role how the methods of artificial intelligence and the distributed infrastructure will be treated. In the future, it will be more important to operate and learn on encrypted data (Smart, 2023) and to use methods such as Fully Homomorphic Encryption (FHE) (Sanon, et al., 2023) in order to take privacy aspects into account, as well.

3. Authentication of Tomorrow: Challenges and Approaches

With the ongoing interconnection and the increasing use of distributed applications, the available authentication options are also changing significantly. Here, the emerging challenges but also innovative approaches in the field of authentication are addressed, especially with regard to the wireless communication of the future, in relation to Beyond 5G (B5G) and the Sixth Generation (6G) (Ruzomberka, et al., 2023) wireless technologies. Machine Learning (ML) approaches as well as Zero Trust Architectures (ZTA) and zero knowledge authentication will also be considered.

3.1 Biometrics: A Step Towards Personalized Security

Biometric authentication is the oldest existing method, but it is not just a human characteristic, even animals can recognize their counterparts by smell, stature and voice (Schneier, 2014). In the meantime, however, this area has developed beyond the traditional methods such as voice, fingerprint or iris pattern and more sophisticated methods are being used. These include the use of bio-electrical signals emitted by the human brain in the form of Electroencephalography (EEG) (Bidgoly, et al., 2020), the volumetric changes of peripheral blood vessels via Photoplethymography (PPG) (Sarkar, et al., 2016) or the use of step and movement patterns recorded by intelligent insoles (Lipps, et al., 2021). While biometrics, which enable the authentication of individuals based on unique personal characteristics, have been acclaimed as a significant advance in security technology, and fundamentally "biometrics are great because they are really hard to forge" (Schneier, 2000), they also suffer from inherent difficulties as they are "lousy [...] (and) easy to forge" (Schneier, 2000). Above all, the emergence of highly developed AI and Deepfake (Chadha, et al., 2021) technologies fostered new vulnerabilities. The ability to imitate voices, facial features and even fingerprints raises serious security concerns and renders traditional biometric methods practically ineffective. In addition, the problem remains that once biometric data has been compromised, it can no longer be used as a feature.

3.2 Physical Layer Security

According to *Lipps and Schotten*, Physical Layer Security (PhySec) comprises “various methods of how to utilize inherently present characteristics of media (hardware, wireless channel and human body) to derive secrets applicable as cryptographic primitives” *(2022)*. Besides "traditional" methods such as Physically Unclonable Functions (PUFs) (Gassend, et al., 2002) -using properties of semiconductor devices and electronic circuits-, and Secret Key Generation (SKG) -using properties of the wireless radio channel-, these also include Human PUFs -properties of the human body; biometrics-. In particular, the so-called 6G-enabling technologies such as Wireless Optical Communication (Wei, et al., 2022), Reconfigurable Intelligent Surfaces (Lipps, et al., 2023) and AI, open up a wide range of possibilities for incorporating these methods into the security and authentication process.

Following *Bruce Schneier's* statement "security is never black and white, and context matters more then technology" (Schneier, 2000), the effectiveness and appropriateness of security measures depends significantly on the context in which they are applied. Different technologies, each with their own strengths and weaknesses, need to be considered as part of a comprehensive security strategy. This approach is crucial for developing systems that are not only secure, but also practical and user-friendly. Precisely the PhySec methods can contribute to this, not only depending on the context, but also as an additional factor, as additional context in MFA applications: If, for example, the MFA can be complemented by characteristics of the wireless channel, which are almost unique in this form, or if a RIS can provide such individual characteristics, then this is a major step towards more secure, plausible and integer authentication.

3.3 Zero Trust Architectures and Zero Knowledge Authentication

The principle of Zero Trust Architecture (ZTA) is becoming increasingly important, especially in the context of the security of the next generation of mobile communications, 6G. *Chen*, for example, emphasizes the importance of ZTA in establishing secure network environments (2023). This approach is based on the assumption that no entity, whether internal or external, is inherently trustworthy - never trust, always verify - even if the entity is already within a trustworthy environment. Authentication is therefore required at every stage of digital interaction.

As the principle of zero trust can be applied to data access and data management, the implementation of privacy-preserving authentication techniques requiring authentication every time data is accessed represents a significant step forward in protecting user data and ensuring secure access (Tang.2023). Especially with regard to corresponding user roles, such as Attribute-Based Access Control (ABAC), in combination with context-based authentication (see above), there are opportunities for innovative solutions.

In addition to ZTA and the basic distrust of entities and access, authentication without a priori knowledge, Zero Knowledge Authentication (ZKA), is a pivotal technology to improve privacy and security, especially in (I)IoT and B5G/6G networks of the future. *Chen's* study highlights the potential of ZKA in digital authentication, which allows credentials to be verified without revealing sensitive information beforehand (2023). Even though the basic principle dates back to the early 1990s (Bellovon & Merritt, 1992), the ZKA addresses the challenges of (I)IoT by authenticating devices and users without compromising their sensitive data. This approach is crucial in networks with extensive data collection and transmission. In particular, due to its efficiency and scalability, ZKA offers advantages that fulfil the requirements of high-performance and densely interconnected environments.

Furthermore, the combination of ZKA with ML (Arp, et al., 2023) increases security by detecting unauthorized access and anomalous behaviour, further enhancing the security of IoT networks. The use of ZKA in IoT and advanced wireless networks is a significant step towards a secure digital ecosystem and meets the growing demand for privacy-friendly and user-friendly authentication solutions.

4. Secure Authentication: An Evaluation

In the dynamic field with a wide range of different authentication methods, the evaluation of security and efficiency is of crucial importance. Based on the previous descriptions, corresponding criteria for a rather objective evaluation of methods are proposed here. Therefore, based on the proposal by *Bonneau, et al.* (2012), a distinction between *usability*, *deployability* and *security,* the principle is extended at this point to encompass the dimensions *continuity* and *adaptability*[2]. As illustrated in Figure 2, authentication primarily needs to be thought of as layers. All domains are important, no doubt, but depending on the use case and available resources, the requirements have to be prioritized as suggested here: The Security & Resilience of the applications ought to be at the core of the requirements. As listed in Table 1, each of these categories consists of a set of relevant requirements. For instance, components such as resilience against leakage, phishing or the guessing of factors, but also cryptographic strength and unlinkability are significant for the Security & Resilience of a system.

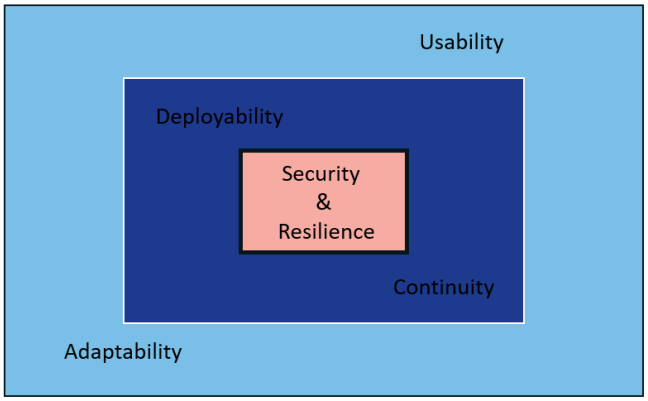

Figure 2: Layered model of the requirements for authentication mechanisms

In a second layer, the requirements for the deployability and continuity of a method are to be considered. This includes, for example, how practical and feasible a method is, but also aspects such as the validity period of a completed authentication or the ability to re-authenticate. The aspects of usability and adaptability can be considered in the outer layer, and thus as merely subordinate and decisive. An overview of the significance of the factors and details regarding their content is provided in Table 1.

[2] Please note: The ranking of components given here is the authors' suggestion; there may be other, individual rankings depending on use cases and available resources;

Table 1: Overview and description of the criteria

Criteria	Description
Security & Resilience	How secure and resilient is a method/system against attacks and intentional and unintentional incidents?
Resilience against compromising (spying, eavesdropping, faking, phishing,…)	Resistance to the loss of a factor through espionage, wiretapping or faking
Resilience against theft	Resistance to compromise through theft of single or multiple authentication factors.
Resilience against guessing and imitation	Resistance to randomness (entropy) and deception
Cryptographic strength	Strength of a method in terms of cryptographic properties such as complexity, computing power and memory
Unlinkability	Inability to determine whether users authenticate themselves multiple times; ability to keep different sessions separate and not linked
Deployablity	How operational is a method in terms of its feasibility and practicability of implementation?
Accessibility	Accessibility for users with different abilities and requirements; loss/restriction of physiological abilities
Maturity of the application	Technical and practical readiness of a system; functional implementation available?
Proprietary application?	Is the method a proprietary system?
Costs caused by the application (time, money, computing power,...)	How expensive is the application in terms of computing power, monetary resources, time for implementation and execution
Continuity	How continuous is the application, particularly in terms of period of validity and combinability
Validity period of authentication	How long is an authentication valid, in which time frame is a new authentication necessary?
Re-authentication capability	Does the method enable re-authentication? How complex/expensive is it?
Combinability with other methods	Can the method be combined with other methods (also in the context of an MFA)?
Usability	How manageable is a method?
Complexity of the method (ability to learn it, complexity of the steps to be completed,...)	Does the method require a complex and elaborate procedure or can it be used by everyone?
Need for additional hardware/tokens/aids	Is anything additional required to use the method, such as hardware or other specialized information?
Adaptability	How adaptable is the method to internal and external influences and current events?
Scalability of the method	How many devices can the method operate, is there an upper limit?
Adaptability to internal and external changes	Can the method react or be adapted to unforeseeable internal/external influences?

In addition to the criteria listed in **Table 1**, there may be others; the list is deliberately designed in such a way that additions can be made at any time. The selection of the superior groups is also not a closed list, although an attempt has been made to define these categories as universally as possible. Current situations and new technological developments lead to further adaptation and integration of the list, this is possible at any time. However, this overview can serve as a starting point, especially with regard to future work. **Table 2** correlates the above criteria with existing authentication methods. The methods were discussed and classified by a panel of experts.

Table 2: Evaluation of the criteria with existing authentication methods

		Passwords, PIN-Codes, Passphrases	Biometics (physiological, behavioural and. biological)	Certificates	Token, Smart-Cards	Trusted Platform Modules, Hardware Security Modules, Physically Unclonable	Zero-Trust Architectures	Zero-Knowledge Authentication	Context (location, date, plausibility, Physical Layer Security Factors)
Security & Resilience	Resilience against compromising	o[3]	✓[3]	o	✓[3]	✓	✓	✓	o
	Resilience against theft	X	✓[3]	X	X	o	✓	✓	✓
	Resilience against guessing and imitation	o[3]	✓[3]	✓	✓	✓	✓	✓	✓
	Cryptographic strength	o[3]	o[3]	✓	✓	✓	-	-	-
	Unlinkability	X	✓	✓	o	✓	-	-	-
Deploy-ability	Accessibility	✓	o	✓	✓	✓	✓	✓	✓
	Maturity of the application	✓	o	✓	✓	✓	o	o	o
	Proprietary application?	X	X	X	X	X	X	X	X
	Costs caused by the application	L	H	M	M	M	M	M	M
Continuity	Validity period of authentication	o	o	L	L	L	-	-	M
	Re-authentication capability	H	H	M	M	H	-	-	H
	Combinability with other methods	H	H	M	H	H	-	-	H
Usability	Complexity of the method	L	M	M	M	H	H	H	M
	Need for additional hardware/tokens/aids	X	X	✓	✓	✓	-	-	✓
Adaptability	Scalability of the method	H	M	H	M	M	H	H	H
	Adaptability to internal and external changes	X	o	X	X	X	-	-	✓

✓= Yes, X = No, o = Medium, M = Medium, L = Low, H = High, - = no consideration

As mentioned, the summary in **Table 2** provides an overview of the different categories of existing authentication groups and the criteria for their use. There is no claim to completeness here, but should serve as a starting point for a deeper analysis of the subject area. The different methods are not always consistent and depend in part on the specific application and method. For example, "Resilience against imitation" is marked as good for biometric methods, although it is well known that there are attacks by deepfakes, for example, or in the knowledge that fingerprints and iris scans have been considered broken for years. However, modern and sophisticated procedures such as gait recognition or EEG are taken into account.

5. Conclusion and Future Work

The future of all of us will be a hyperconnected future. Above all, we will be able to perceive the effects clearly in everyday applications such as autonomous driving, medical applications and living in the metaverse. But as not only the amount of data will increase significantly, but its content and value will gain in importance, its integrity and security will be more crucial than ever before. The insight given into the multifaceted field of authentication highlights that the evolution towards secure, efficient and user-friendly authentication is an ongoing and evolving challenge. Technological advances, particularly in the fields of (Industrial) Internet of Things, biometrics, Machine Learning and next-generation wireless systems, are opening up new opportunities for innovative authentication methods. Nevertheless, these developments come along with complexities and vulnerabilities which need to be addressed as well. Upcoming trends such as Zero Trust Architecture and Zero Knowledge Authentication are an essential step towards a stronger digital environment. These approaches are

[3] Depending on the specific application and use case; may differ

in line with the growing importance of privacy and data protection in our increasingly interconnected world. They offer robust solutions against a wide range of cyber threats, but their implementation requires a change in traditional security paradigms and user behaviour. The experience gathered demonstrates that no single authentication method can overcome all security and usability concerns: A hybrid approach combining different, situation-adapted methods to balance usability, security and privacy is certainly the most promising and effective approach. This adaptable and context-sensitive strategy is crucial in a world where digital interactions are becoming increasingly complex and integral to our daily lives. Therefore, the future of authentication depends on continuous innovation and adaptation. Building solutions that are not only technologically advanced, but also ethically sound and user-centred, will require a collaborative effort between technologists, security experts, policy makers and users. In navigating this constantly changing environment, we must continue to focus on creating a secure, efficient, and inclusive hyperconnected world for all of us.

Acknowledgement

This work has been supported by the Federal Ministry of Education and Research of the Federal Republic of Germany (Förderkennzeichen 16KIS1841K ALPAKA and 16KIS1283 AI-NET PROTECT). The authors alone are responsible for the content of the paper.

References

Arp, D., Quiring, E., Pendkebury, F., Warnecke, A., Pierazzi, F., Wressnegger, C., Cavallaro, L., and Rieck, K., "Lessons Learned on Machine Learning for Computer Security", *IEEE Security & Privacy, vol.* 21, no. 5, pp. 72 --77, DOI: 10.1109/MSEC.2023.3287207, 2023.

Bellovon, S. and Merritt, M., "Encrypted key exchange: password-based protocols secure against dictionary attacks", *IEEE Computer Society Symposium on Research in Security and Privacy,* Oakland, CA, USA, DOI: 10.1109/RISP.1992.213269, *1992*.

Bidgoly, A. J., Bisgoly, H. J. and Arezoumand, Z., "A survey on methods and challenges in EEG based authentication", *Computers & Security,* Band 93, DOI: 10.1016/j.cose.2020.101788, 2020.

Bonneau, J., Herley, C., van Oorschot, P. and Stajano, F., "*The Quest to Replace Passwords: A Famework for Comparative Evaluation of Web Authentication Schemes" IEEE Symposium on Security and Privacy*, San Fransisco, CA, USA, DOI: 10.1109/SP.2012.44, 2012.

Burrows, M., Abadi, M. and Needham, R., "A logic of authentication" *ACM Transactions on Computer Systems, vol.* 8, no. 1, pp. 18 -- 36, DOI: 10.1145/77648.77649, 1990.

Burr, W.E., Dodson, D.F., Newton, E.M., Perlner, R.A., Polk, W.T., Gupta, S., and Nabbus, E.A., "NIST Special Publication 800-63-2 - Electronic Authentication*", National Institute of Standards and Technology,* 2013.

Campisi, P., "Security and Privacy in Biometrics"*,* 1st Edition, Springer London, ISBN: 978-1447152293, 2013.

Chadha, A., Kumar, V., Kashyap, S. and Gupta, M., "Deepfake: An Overview", *Proceedings of Second International Conference on Computing, Communications, and Cyber-Security,* DOI: 10.1007/978-981-16-0733-2_39, 2021.

Ciocarlie, G.F. and Zhou, J., "Securing Critical Infrastructure Across Cyber and Physical Dimensions", *IEEE Security & Privacy, vol.* 21, no. 4,, DOI: 10.1109/MSEC.2023.3282424, 2023.

Cisco, "Cisco Annual Internet Report (2018–2023)*", White Paper,* 2020.

Garman, J., "Kerberos: The Definitive Guide"*,* 1. Edition, O'Reilly & Associates, 2023.

Gassend, B., Clarke, D., van Dijk, M. and Devadas, S., "Silicon Physical Random Functions", *Proceedings of the 9th ACM Conference on Computer and Communication Security*, pp. 148 -- 160, DOI: 10.1145/586110.586132 2002.

Ho, L.K. and Katuk, N., "Social login with OAuth for mobile applications: User's view"*, IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE),* Penang, Malaysia, DOI: 10.1109/ISCAIE.2016.7575043 , 2016.

Huseynov, E. and Seigneur, J.-M., "Context-Aware Multifactor Authentication Survey", In: M. Kaufmann, Hrsg. *Computer and Information Security Handbook.* Third Edition, Boston, USA, pp. 715 -- 726, DOI: 10.1016/B978-0-12-803843-7.00050-8, 2017.

Kimovski, D., Mathá, R., Hammer, J., Mehran, N., Hellwagner, H. and Prodan, R., "Cloud, Fog, or Edge: Where to Compute?", *IEEE Internet Computing, vol.* 25, no. 4, pp. 30 -- 36, DOI: 10.1109/MIC.2021.3050613, 2021.

Lin, J., Xu, L., Liu, Y. and Zhang, X., "Composite Backdoor Attack for Deep Neural Network by Mixing Existing Benign Features", *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security,* pp. 113 -- 131, DOI: 10.1145/3372297.3423362, 2020.

Lipps, C., Baradie, S., Herbst, J., Armistead, L., and Schotten, H.D., "Cybersecurity in Industrial Automation and Control Systems: The Recent Attack of the Colonial Pipeline", In: Van Niekerk, B., Ramluckan, T. and Kushwaha, N., *Modelling Nation-state Information Warfare and Cyber-operations.* United Kingdom: Academic Conferences and Publishing International Limited, pp. 215 -- 236, ., 2022.

__, Baradie, S., Noushinfar, M., Herbst, J., Weinand, A., and Schotten, H.D., "Towards the Sixth Generation (6G) Wireless Systems: Thoughts on Physical Layer Security", *Mobile Communication - Technologies and Applications - 25. VDE/ITG Fachtagung Mobilkommunikation*, Osnabrück, Germany, 2021.

__, Herbst, J., Klingel, S., Franke, S., Wolff, A., Rüb, M., Reddy, R., Rahm, M., and Schotten, H.D., "Connectivity in the era of the (I)IoT: About Security, Features and Limiting Factors of Reconfigurable Intelligent Surfaces", *Discover the Internet of Things, vol.* 3, no. 16, DOI: 10.1007/s43926-023-00046-1, 2023.

__, Herbst, J., and Schotten, H.D., "How to Dance Your Passwords: A Biometric MFA-Scheme for Identification and Authentication of Individuals in IIoT Environments", *16th International Conference on Cyber Warfare and Security (ICCWS)*, Cookeville, TN, USA, DOI: 10.34190/IWS.21.016, 2021.

__, and Schotten, H.D., "Physical Layer Security: About Humans, Machines and the Transmission Channel", *21st European Conference on Cyber Warfare and Security (ECCWS2022),* Chester, United Kingdom, DOI: 10.34190/eccws.21.1.403, 2022.

__, Tjabben, A., Rüb, M., Herbst, J., Sanon, S.P., Reddy, R., Munoz, Y., Schotten, H.D., "Designing Security for the Sixth Generation: About Necessity, Concepts and Opportunities", *22nd European Conference on Cyber Warfare and Security*, Academic Conferences International, Athens, Greece, DOI: 10.34190/eccws.22.1.1207, 2023.__, Weinand, A., Krummacker, D., Fischer, C., and Schotten, H.D., "Proof of Concept for IoT Device Authentication Based on SRAM PUFs Using ATMEGA 2560-MCU*", 1st International Conference on Data Intelligence and Security (ICDIS)*, South Padre Island, TX, USA, DOI: 10.1109/ICDIS.2018.00013, 2018.

Ma, C., Li, J., Wei, K., Liu, B., Ding, M., Yuan, L., Han, Z., and Poor, H.V., "Trusted AI in Multiagent Systems: An Overview of Privacy and Security for Distributed Learning", *Proceedings of the IEEE, vol.* 111, no. 9, pp. 1097 -- 1132, DOI: 10.1109/JPROC.2023.3306773, 2023.

Needham, R.M. and Schroeder, M.D., "Using encryption for authentication in large networks of computers", *Communications of the ACM, vol.* 21, no. 12, pp. 993 -- 999, DOI: 10.1145/359657.359659, 1978.

O'Gorman, L., "Comparing passwords, tokens, and biometrics for user authentication" *Proceedings of the IEEE, vol.* 91, no. 12, pp. 2021 -- 2040, DOI: 10.1109/JPROC.2003.819611, 2003.

Otway, D. and Rees, O., "Efficient and timely mutual authentication", *ACM SIGOPS Operating Systems Review, vol.* 21, no. 1, pp. 8 -- 10, DOI: 10.1145/24592.24594, 1987.

Radha, V. and Reddy, D.H., "A Survey on Single Sign-On Techniques", *Procedia Technology,* Band 4, pp. 134 -- 139, DOI: 10.1016/j.protcy.2012.05.019, 2012.

Ruzomberka, E., Love, D.J., Brinton, C.G., Gupta, A., Wang, C.-C., and Poor, H.V., "Challenges and Opportunities for Beyond-5G Wireless Security", *IEEE Security & Privacy, vol.* 21, no. 5, pp. 55-66, DOI: 10.1109/MSEC.2023.3251888 2023.

Sanon, S. P., Lipps, C. and Schotten, H.D., "Fully Homomorphic Encryption: Precision Loss in Wireless Mobile Communication", *Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit),* Gothenburg, Sweden, DOI: 10.1109/EuCNC/6GSummit58263.2023.10188286, 2023.

Sarkar, A., Abbott, A.L. and Doerzaph, Z., "*Biometric authentication using photoplethysmography signals", IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS),* Niagrara Falls, NY, USA, DOI: 10.1109/BTAS.2016.7791193, 2016.

Schneier, B., "Secrets & Lies - Digital Security in a Networked World",. 1st Edition, New York: John Wiley & Sons, Inc., 2000.

__, "Liars & Outliers - Enabling the Trust that Society need to thrieve", 1st Edition, Indianapols: John Wiley & Sons, Inc., 2012.

__, "Carry On: Sound Advice from Schneier on Security". 1st Edition, Wiley, 2014.

__, "Applied Cryptography: Protocols, Algorithms and Source Code in C", 25th Anniversary Edition, John Wiley & Sons Inc., 2015.

Smart, N., "Computing on Encrypted Data", *IEEE Security & Privacy, vol.* 21, no. 4, pp. 94-98, DOI: 10.1109/MSEC.2023.3279517, 2023.

Tolanur, J. and Chaudhari, S., "DDoS Attacks Analysis with Cyber Data Forensics using Weighted Logistic Regression and Random Forest", *International Conference on Device Intelligence, Computing and Communication Technologies (DICCT),* Dehradun, India, DOI: 10.1109/DICCT56244.2023.10110133 , 2023.

Tolpegin, V., Truex, S., Gursoy, M.E. and Liu, L., "Data Poisoning Attacks Against Federated Learning Systems", *European Symposium on Research in Computer Security,* pp. 480 -- 501, 2020.

Tuptuk, N., Hazell, P., Watson, J. and Hailes, S., "A Systematic Review of the State of Cyber-Security in Water Systems", *Water, vol.* 13, no. 81, DOI: 10.3390/w13010081, 2021.

Wei, Z., Wang, Z., Zhang, J., Li., Q., Zhang, J., and Fu., H.Y., "Evolution of optical wireless communication for B5G/6G", *Progress in Quantum Electronics,* Band 83, DOI: 10.1016/j.pquantelec.2022.100398, 2022.