Received January 10, 2022, accepted January 21, 2022, date of publication February 7, 2022, date of current version February 15, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3149475

E-Banking Security Study–10 Years Later

KAMIL MALINKA, ONDŘEJ HUJŇÁK, PETR HANÁČEK, AND LUKÁŠ HELLEBRANDT
Faculty of Information Technology, Brno University of Technology, 612 00 Brno, Czech Republic

Corresponding author: Kamil Malinka (malinka@fit.vutbr.cz)

This work was supported by the Internal Project of Brno University of Technology (BUT) under Grant IGA FIT-S-20-6427.

ABSTRACT ICT security in the banking area is going through rapid changes. It is ten years since we covered the state of e-banking security, and both authentication schemes and legislation has evolved. With the Payment Services Directive (PSD2) for European Union coming into force, we believe it is a good time to update our findings. PSD2 brings new requirements for multi-factor authentication, thus it is necessary to revise compliance of currently used schemes. This work's main contribution is an overview of current authentication methods, their properties with respect to international standards, and their resistance against attacks. We further discuss the multi-factor authentication schemes composed of those methods and their compliance with the PSD2 requirements. In order to present the overview, we introduced the e-banking attacks taxonomy, which is compatible with authenticator threats from NIST Digital Identity Guidelines but has an increased level of detail with respect to the e-banking area. The available sources in this area are usually either very broad, targeted on the business executive, or focus on one particular issue or attack in greater detail. We believe our article can bridge such diverse sources by providing a comprehensive and complex tool to help with orientation in the area.

INDEX TERMS Online banking, PSD2, authentication, multi-factor, cybersecurity, secure hardware.

I. INTRODUCTION

Ten years ago, we published a comparative study focused on the security of e-banking [1], where we summarised basic forms of electronic banking and widely used authentication and authorisation methods. Given the drastic evolution of the situation over the years, shift to mobile banking and the emergence of new European directives that affect this area, we believe it is an ideal time to update our findings. Changes in user behaviour and used equipment directly impact the security of the whole environment. For example, by integrating smart banking into the smartphone, we are losing a secure second channel used for SMS verification, as opposed to the traditional web application e-banking performed through a PC (i.e., second channel). Also, the ''smartness'' of the devices brings new vectors of attacks as they can be targeted by malware.

The goal of this paper is to present an overview of current authentication methods, their relation to the most common attacks on electronic banking and the level of protection they can provide. With new requirements on two-factor authentication brought by the new European directive PSD2, we also discuss possible combinations of authentication methods and evaluate their usability and security properties.

A. PARADIGM SHIFT

The banking sector keeps going through continuous digital evolution as the paradigms in the finance sector are shifting. Ten years ago, we witnessed the transfer from in-person banking to online e-banking, and this trend continues towards mobile banking. Moreover, with the increase of accessibility and digitisation of services, fully digital banking emerged and, in such an environment, physical contact with the customer is completely dropped in favour of digital means.

SwissFinanceCouncil estimates that nearly 60% of retail banking transactions worldwide go through mobile and online channels [2]. This corresponds with reports from other countries such as Brazil [3] as shown in Figure 1, where digital channels carry out 63% of banking transactions (either mobile or internet banking) and the share of mobile banking is increasing every year. The shift towards mobile solutions is apparent also in the Deloitte GMCS report, which claims that according to the UK survey, a smartphone is a device of preference when using banking services for the majority of people [4].

The associate editor coordinating the review of this manuscript and approving it for publication was Weizhi Meng.

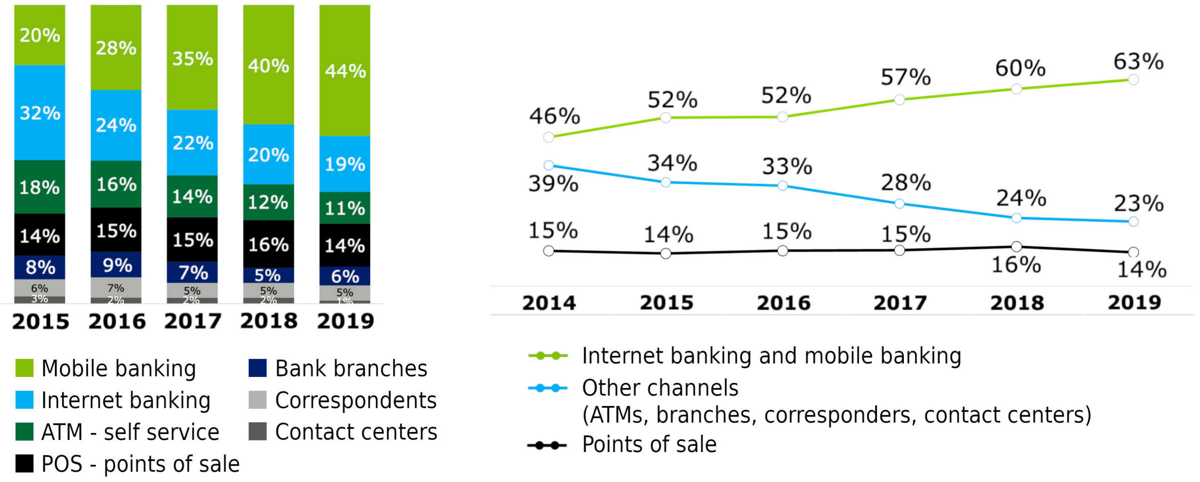


FIGURE 1. Composition of banking transactions in Brasil (in %) [3].

The popularity of mobile banking corresponds with the adoption of smartphones and, as noted by Pew Research Centre, "today, most people who own a mobile phone own a smartphone" [5]. The users of basic cell phones, which were targeted as 2nd factor for e-banking ten years ago, are rapidly decreasing. Also, in advanced economies, only 18% of people own a basic cell phone, as seen in Figure 2.

These changes bring not only increased comfort to the users but impose new security challenges on the banks. The worldwide spread of FinTech services as observed by EY [6] brings further focus on using emerging technologies to provide financial operations that rapidly expand the attack surface. One of the most eminent new challenges is identity verification in fully digital banking.

When facing these challenges, financial institutions were forced to develop new mitigation techniques and update the legacy ones. The identity and operation verification shifted to enforce multi-factor authentication with various factors. While the passwords and PIN codes are still broadly used, authentication calculators were superseded by SMS codes, which are now replaced by newly established factors such as digital tokens and biometrics. For payment card operations, 3D Secure protocol [7] was introduced.

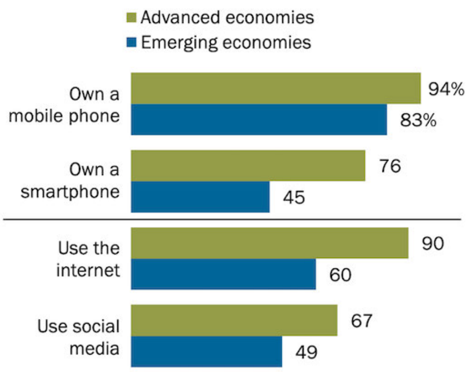


FIGURE 2. Mobile technology, internet, and social media use [% of adults] [5].

New legislation frameworks were developed to establish interoperability and security across the financial sector and updated to address emerging concerns. The international standard addressing security is Payment Card Industry Data Security Standard (PCI DSS [8]), while the European Union introduced a significant change in approach with its Payment Services Directive version 2 (PSD2) [9]. PSD2 forces financial institutions to publish interface to their data, effectively allowing FinTech companies to work with it. To ensure security, PSD2 dictates strong authentication and multi-factor authentication.

B. CONTRIBUTIONS

The main contribution of this paper lies in the security evaluation of authentication schemes composed of viable combinations of authentication methods concerning the concurrent standards - mostly the PSD2 directive of the European Union. In order to perform this evaluation, we propose a specific e-banking attacks taxonomy and define authentication primitives and their security features.

All contributions of the paper can be summarised as follows:

- We propose e-banking attacks taxonomy compatible with authenticator threats from NIST Digital Identity Guidelines, but with an increased level of detail with respect to the e-banking area. In taxonomy, we describe relevant attacks and trends in their occurrence. We look in more detail at the two most common types of attacks – phishing and malware.
- We present an overview of current authentication methods and their properties in the context of international standards. We also benchmark their resistance against attacks from taxonomy.

- We introduce possible combinations of the multi-factor authentication schemes composed of current authentication methods and evaluate their compliance with the newest standard available – the PSD2 directive of the European Union.
- We address future trends and present open gaps.
- We provide up to date and comprehensive view of e-banking security, enabling the reader to get an overview of available options and their advantages and disadvantages in the context of current international regulations.

C. ORGANIZATION

The rest of the paper is organised as follows: In Section II, we present e-banking attacks taxonomy with the description of attacks, their impact and historical context. In greater detail, we focus on malware and phishing, which are currently the most common. In Section III, we explain elementary authentication primitives and their properties with respect to the requirements from NIST and PSD2. To increase the detail for the e-banking area, we have expanded the former categories into multiple subcategories and discuss their resistance to attacks from our taxonomy. We discuss the usability of multiple factors combination in the context of new PSD2 requirements in Section IV. Then, in Section V we summarize related work. Finally, in Section VI, we conclude the paper.

II. ATTACKS ON E-BANKING SYSTEMS

This section presents an overview of the current attacks on e-banking and their trends. We identify which attacks are declining in their usage and which are emerging thanks to the new technologies used nowadays and a shift in user behaviour.

A. PROPOSED E-BANKING ATTACK TAXONOMY

E-banking security is a well-known research topic, and many scientific papers and studies can be found (eg. [10]–[13] [14], [15]). The main issue of these sources is that they often focus on very specific attacks (mostly scientific papers) or broadly cover the topic for business executives. Thus, we decided to create a reference taxonomy, which can be used to ease orientation in the broad spectrum of e-banking attacks.

The proposed e-banking attack taxonomy, shown in Figure 3, defines four most common categories:

- ***Authentication and authorisation attacks*** – Goal of attacker is to obtain valid user credentials (such as passwords, PINs, certificates etc.) for a specific service.
- ***Identity theft (identity stealing)*** – In these attacks, the adversary attempts to misuse or take over someone's identity to enable various malicious behaviour.
- ***Communication attacks*** – Attacks that passively listen to communication between two parties or actively transparently participate in it.
- ***Attacks focused on bank*** – For the sake of comprehensive overview, we add the category of attacks directly targeting bank infrastructure and bank employees as opposed to previous categories focusing on users (bank clients) and their communication channels.

  These attacks represent a high risk, high value for attackers as successful attacks of this category can cause financial gain in hundreds of millions of dollars. However, they are hard to carry out because banking infrastructure protection usually uses state of the art technologies. A deeper study of this category is beyond the scope of this article.

The category list we propose is not exclusive by nature. As some attack types may fall into various categories depending on the point of view used, the defined categories blend seamlessly. We have subdivided every category into specific attack techniques that fulfil the malicious goal of the category. The full proposed taxonomy is displayed in Figure 3, and the description of individual elements follows:

A-1 Authentication and Authorisation Attacks

The attacker's goal is to obtain valid user credentials (such as passwords, PINs, certificates, etc.) for a specific service.

A-1.1 Password Guessing

Password guessing is an attack based on systematic guessing of a user password. There are multiple approaches, such as a dictionary-based attack, brute-force, or even attacks based on neural network usage [16].

There are three main approaches used for e-banking attacks: first mentioned above, second uses guessing of one high-quality password which is then used on a large number of clients (because it is unfeasible to test a large number of passwords on one user account). The third approach uses a password obtained from other sources of leaked passwords.

A-1.2 Exhaustive Search

Known also as a brute force attack is based on trying a large number (all) possible passwords or secret values. This approach is not commonly used in the banking environment due to the limited attempts and difficulty of obtaining an encrypted password file. However, it is viable to crack passwords from leaked credential databases or other sources and use those against bank authentication. Distributed high-performance computing can be used to increase attack speed [17].

A-1.3 Phishing

Phishing tries to deceive the user by fraudulent e-mail/webpage to steal credentials or other personal data [18]. Targeting the user as the weakest link has proved to be a very dangerous and successful technique.

A-1.4 Pharming

This technique is similar to phishing but usually requires the assistance of malware or DNS spoofing attacks which redirect users to fake sites with

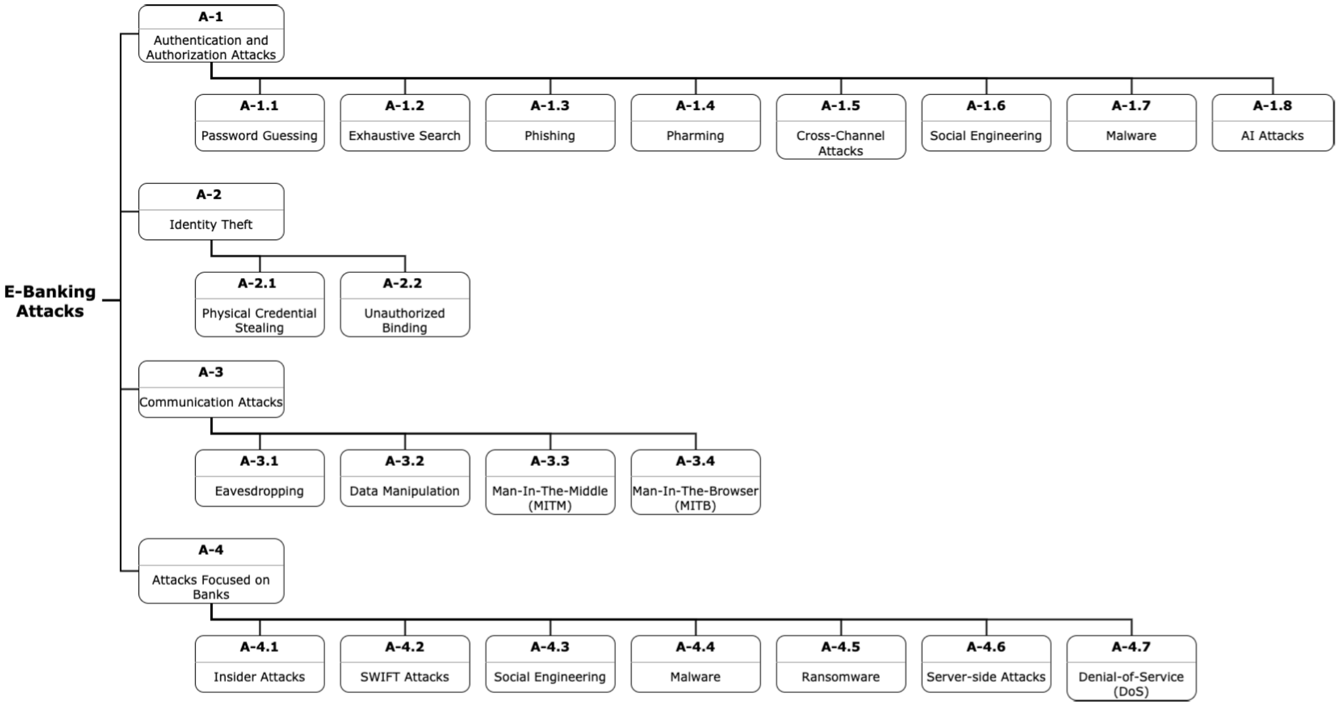


FIGURE 3. E-banking attacks taxonomy.

a similar appearance as original pages (bank pages etc.) [19], [20].

A-1.5 Cross-Channel Attacks
These attacks usually target systems that use multi-factor authentication (2FA), where the adversary is forced to attack multiple channels simultaneously, e.g., a simultaneous attack on internet connection and SMS messages. Attacking multiple channels usually requires various methods, such as a combination of social engineering and hacking.

A-1.6 Social Engineering
Social engineering is a way of manipulating people, so they give up confidential information, which includes passwords, bank information, or access to a computer to install malicious software secretly.

A-1.7 Malware
Specialized malware that is designed for credential stealing [21]. The most common class is the banking trojan which advertises itself as a useful application while scraping credentials or supporting other attacks in the background. Modern malware is multi-purpose, and there is malware for both computer and mobile OS's.

A-1.8 AI Attacks
Attacks specialise exclusively on (biometric) authentication, usually in the context of the "Know Your Customer" (KYC) process, such as creating fake samples to deceive voice and face recognition systems. Attackers can utilise an algorithm class called generative adversarial network (GAN), which is a class of machine learning algorithms designed to generate artificial data with the same statistics as the training set [22]. An example of the exact use of GAN is false eye image creation [23].

A-2 Identity Theft
The goal of the attacker is to misuse or take over someone's identity to enable various malicious behaviours.

A-2.1 Physical Credential Stealing
Real-world theft of ID cards or creating counterfeit documents with high value to criminals such as passports, driver licenses, credit cards, bank statements, tax statements, medicare cards and utility bills.

A-2.2 Unauthorised Binding
Unauthorised Binding is a class of attacks aiming to bind an adversarial authentication device (such as HW token, SIM card or private key) to the victim's account. Because of the common usage of SMS codes as an out-of-band (oob) second factor, the most relevant attacks are aimed at telecommunication operators (telco). We provide examples of two such attacks – SIM Swapping and SS7 attacks. SIM Swapping is a technique for diverting telco services (including calls and SMS) from victims' mobile carrier account to a new SIM card controlled by an adversary [24]. Similarly, SS7 attacks divert telco services to an attacker, but those attacks

follow the Man-in-the-middle (MITM) scheme and abuse directly vulnerabilities in Signalling System 7 (SS7) protocols used for public telephone calls [25].

A-3 Communication Attacks
Attacks that passively listen to communication between two parties or actively and transparently participate in it.

A-3.1 Eavesdropping
Passive listening to some communication that is happening on a network of any kind without generating any activity – e.g., running a piece of software on a network device, which is merely saving all the data that has passed through it. The collected data, either encrypted or unencrypted, is later analysed and can be further used by the attacker [26]–[29].

A-3.2 Data Manipulation
In Data Manipulation, the adversary not only listens to communication but also actively modifies the messages [30]–[32].

A-3.3 Man-In-The-Middle (MITM)
In Man-in-the-middle, the adversary hijacks the whole communication channel and positions themself in the middle of the communication in order to gain access to the data the communicating parties wouldn't reveal voluntarily [33], [34]. In encrypted communication, the adversary creates encrypted channels to both communicating parties and decrypts and re-encrypts all the messages [35].

A-3.4 Man-In-The-Browser (MITB)
The Man-in-the-Browser attack corresponds to a Man-in-the-middle attack, but in this case, the attacking malware is embedded within a web browser [36].

A-4 Attacks Focused on Banks
Attacks targeting banking organisations with various goals such as theft, data breach, disruption, and espionage.

A-4.1 Insider Attacks
An insider threat is a security risk that originates within the targeted organisation. This doesn't mean that the actor must be a current employee or officer in the organisation. It can be an outsider who positioned himself within an organisation infrastructure [37].

A-4.2 SWIFT Attacks
SWIFT (Society for Worldwide Interbank Financial Telecommunications) is a bank-to-bank electronic messaging system that is the primary means of communication for international wire transfers. These attacks exploit vulnerabilities in the SWIFT interface system allowing the attackers to gain control of the banks' legitimate SWIFT credentials or endpoint device [11]. This leads to sending fake SWIFT funds transfer requests to other banks [38].

A-4.3 Social Engineering
As mentioned above (A-1.6), but with respect to a different environment – focused on bank employees to disrupt trustworthy bank operations. The goal is to convince a bank employee to perform an illegitimate action, e.g. create a forged transaction, reveal private information.

A-4.4 Malware
Specialised malware targeting the bank IT infrastructure [39]. Because banks are usually well protected, this type of malware is usually a custom made and highly sophisticated product of an organised group.

A-4.5 Ransomware
Ransomware is a category of malware able to encrypt the user data and prevent the user from accessing it, thus attacking the availability and causing DoS [40]. The attacker then demands a ransom from the victim to restore access to the data upon payment.

A-4.6 Server-side Attacks
Attacks launched directly from an attacker (the client) to a listening service. Web application attacks are dominant these days, as described by OWASP [41] such as SQL injection, cross-site scripting, broken authentication and session management etc. [42].

A-4.7 Denial-of-Service (DoS)
The DoS attack will send multiple requests to the attacked web resource to exceed the website's capacity to handle multiple requests and prevent the website from functioning correctly [43], [44].

The attack grouping in our taxonomy is compatible with NIST "Digital Identity Guidelines" [45] and provides a deeper focus on the e-banking area. Some NIST threat groups are directly corresponding with attacks we have identified - *Social Engineering*, *Eavesdropping* and *Unauthorised Binding*. For a deeper understanding, we name the password attacks differently than NIST - we use the term *Password Guessing* for *Online Guessing* and *Exhaustive Search* for *Offline Cracking*. We consider *Duplication* a special case of *Theft* and call the group *Physical credential stealing*. Because *Phishing* and *Pharming* attacks have different implications as pharming needs additional supporting malware, we have decided to split them. We consider the groups *Assertion Manufacture or Modification* and *Endpoint Compromise* too general and divide them into more specific groups – *Data manipulation*, *Man-in-the-middle*, *Man-in-the-browser* and *Malware*. A special case is our group *Cross-channel attacks*, which may correspond with both *Eavesdropping* and *Endpoint Compromise* NIST groups depending on the execution of the attack. We define a new group *AI attacks* (Artificial Intelligence attacks) for novel attacks utilising AI to bypass security defences (focused on biometric systems). Lastly, we omit the *Side Channel Attacks* because the extraction of secrets from authenticator is for e-banking security in principle the same as *Physical credential stealing*.

B. OVERALL TRENDS OF ATTACKS

To provide additional value and insight, we attempted to include a recent trend for every attack identified, but this was proven tricky due to the lack of consistent long-term data. Available data from reports usually focus only on the most relevant attacks in the selected time period. Thus, it is not possible to create such trends for a wider range of attacks over the years. Instead, we decided to present an excerpt of findings, which we consider the most important:

- "*Financial services firms fall victim to cybersecurity attacks 300 times more frequently than businesses in other industries*" [10].
- "*Attacks on this sector accounted for 17 percent of all attacks in the top 10 attacked industries*" [47].
- "*Number of security incidents in this sector has tripled in the past five years*" [10].
- "*Social engineering remains the number one threat in breaching security defences, regardless of the maturity and frequency of security awareness campaigns*" [48], [49].
- "*Denial of service, social engineering, drive-by downloads and phishing to disseminate banking Trojans, and malicious insiders remain the most prevalent attack strategies*" [10].

One of the reasons for the increasing number of attacks is their availability and accessibility, even for people without deep knowledge. Many attack tools, especially malware [50] (even zero-day exploits) and phishing kits [51] are available for purchase on dark web marketplaces [52].

Some attacks are very stable in time, and their evolution follows the development of countermeasures, such as phishing and Man-In-the-Middle (MITM). On the other hand, some are brand new, often enabled by new technologies, e.g., mobile malware or Man-In-The-Browser (MITB). Brand new possibilities for attacks are introduced by the increased use of Artificial Intelligence (AI) both in production systems and attack tools. Even though AI attack surfaces are just emerging, Accenture warns that security strategies have to focus on strengthening their critical AI models. Those models are becoming more and more complex, which increases the risk of an adversary discovering a particular behaviour of the model leading to its exploitation [53].

In a historical context, we can also state some additional trends. Because the risk of phishing and other forms of social engineering is too high, the standalone password-based authentication disappeared. The old generation of One-Time Password (OTP) hardware tokens is quickly diminishing, and because of PSD2, there is a trend in the decreasing number of areas where SMS codes are still applicable for authentication, because in some cases (e.g., banking app and SMS on the same smartphone) SMS no longer provides a secure external channel. PKI has changed its role (user software for endpoint authenticators was abandoned and replaced by usage of TLS and some token authentication schemes). We are also awaiting the spread of a new generation of authentication tokens (based on Universal 2nd Factor – U2F, using Trusted Execution Environment – TEE and wireless communication via Bluetooth or NFC).

In the subsections II-C and II-D we focus on two main attack areas, which we consider the most significant – phishing and malware. The significance of these areas is supported by IBM Threat Intelligence Index [47] and Organization of American States (see Figure 4). Even though both are not new in principle and have been used a decade ago, they have both undergone a big evolution and are still the most serious threat in the sector.

C. PHISHING STILL ON THE RISE

Since the first description of this concept in 1987, phishing has become a well-known social engineering technique for user data exfiltration. Even though the principle hasn't changed, phishing campaigns nowadays are more sophisticated and subliminal than people only ten years ago could imagine. In 2001 phishing campaigns started targeting online payment systems, and its share has increased since. The graph in Figure 5 describes the share of financial (and bank) phishing out of all phishing e-mails detected by Kaspersky Labs. The global reach of phishing attacks is also shown in a longitudinal study by Thomas *et al.* [21].

The main development in financial phishing lies in the use of advanced techniques to imitate official correspondence and exploit user gullibility. Modern phishing e-mails are almost indistinguishable from original e-mails thanks to flawless translations, convincing information and carefully crafted landing pages with nearly identical URLs, often with valid HTTPS certificates. A special category of phishing called "spear phishing" keeps growing. Spear phishing campaigns are strictly targeted at a single user or company, allowing attackers even deeper impersonation of valid correspondence. Spear phishing is used to target companies and their financial departments or as a part of the deployment phase of Advanced Persistent Threats [59].

D. MALWARE NEVER DISAPPEARED

Malware (compound of words *malicious* and *software*) is a general term describing software developed with the intent of harming and exploiting the user and his resources. Since the first malware in 1971, it has undergone significant evolution and remains a constant threat even in the financial market.

Computer malware is a broad set of harmful software targeting operating systems and desktop computer users. Traditional categories are *virus*, *worm*, *trojan*, *rootkit* and *spyware*, but modern malware blurs the differences between them, so novel taxonomies based on behaviour have been created [12], [13], [60].

Modern malware is usually a complex piece of software able to launch or support multiple attacks, including

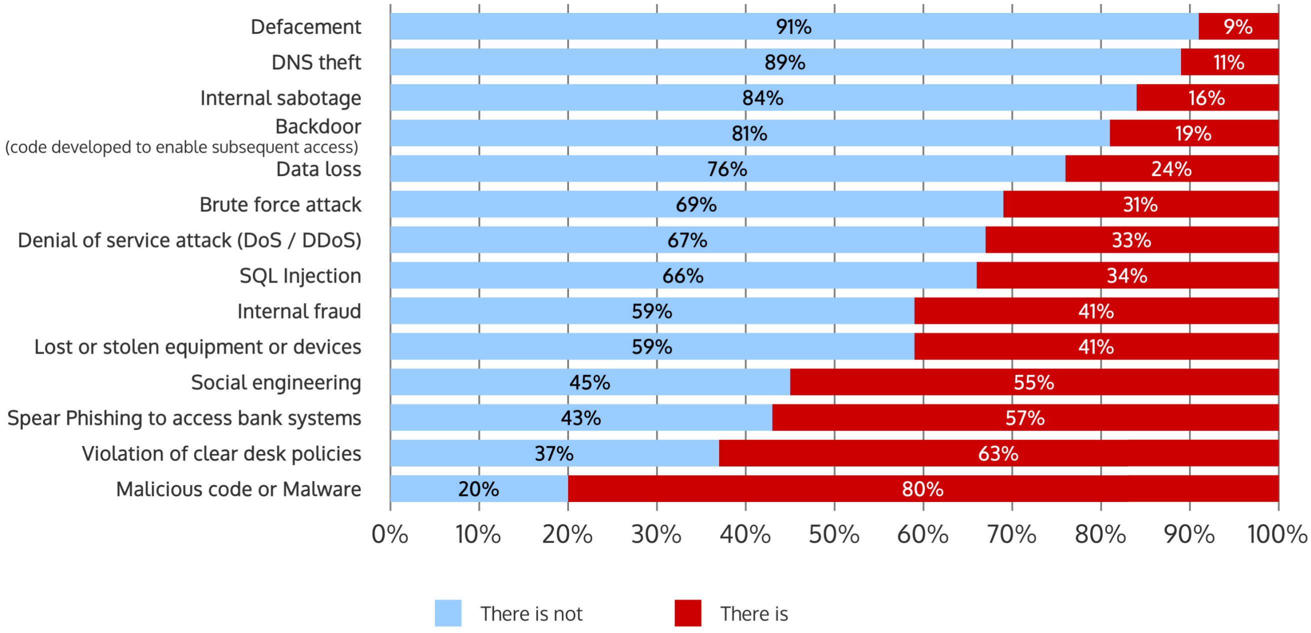


FIGURE 4. Digital security events against banking entities in 2018 in Latin America and the Caribbean [46].

attacks on bank infrastructure, full user simulation or turning the infected system into a remote-controlled bot. Moreover, concurrent malware is often able to deliver additional malware as payload [14]. The development of novel malware never ceases, as is demonstrated in Figure 6 and its detection and mitigation is a never-ending process. We can also notice that recently banking trojans and ransomware have gained popularity, and thus the development of malware from those categories is on the rise.

With the increased versatility and capabilities of mobile phones emerged malware tailored for mobile devices. At first, its use was limited to sending or intercepting messages, but with mobile operating systems (Android, iOS) mobile malware skyrocketed with capabilities similar to computer malware [61]. To describe differences in mobile financial malware more in-depth, Kadir *et al.* suggest a taxonomy of financial malware attacks [15].

Because of the popularity and openness of the Android OS, it became a major target of mobile malware. Android banking trojans are usually injected into a phone by malicious SMS, URL or third-party app stores and installed as APK. Despite all implemented countermeasures, they can also appear in the official app store (Google Play). After installation, they set themselves as a default SMS app or use Accessibility Services to intercept messages (2FA bypass), display phishing screen overlays for banking apps or extract information.

Even though iOS uses a closed ecosystem and APIs, which limit the attack vector for malware at the cost of accessibility and auditability, it is not free of malware as well [62], [63]. But the share of iOS malware is marginal compared to Android because of the difficult spread (tightly controlled App Store) and smaller user base, especially in countries most affected by mobile malware.

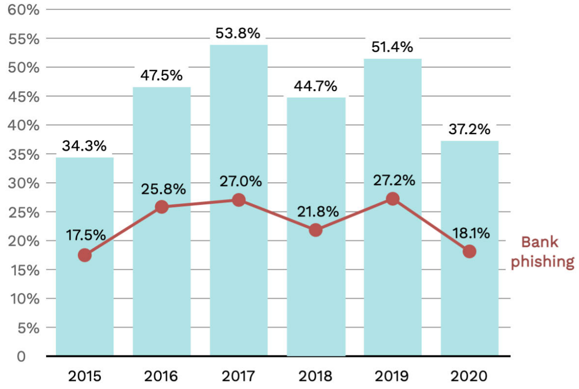


FIGURE 5. Financial phishing share [54]–[58].

The evolution of banking malware led from personal computers targeted malware in 2010 to mobile malware nowadays, thanks to the spread of smartphones and the increasing use of mobile banking. Over the years, the number of people affected by mobile banking malware has skyrocketed and is now catching up with (and sometimes surpassing) computer malware (see graph in Figure 7), so it must be taken into consideration. Malware in general also evolved from single-purpose tools to versatile pieces of code capable of multiple attack scenarios and downloading additional modules or different malware.

In 2018 users affected by Android malware spiked, which was caused mainly by three banking trojan families – Asacub, Agent and Svpeng [56]. The probable reason for this spread is the novel use of DNS hijacking in Android attacks and misuse of Accessibility Services giving the malware superior possibilities.

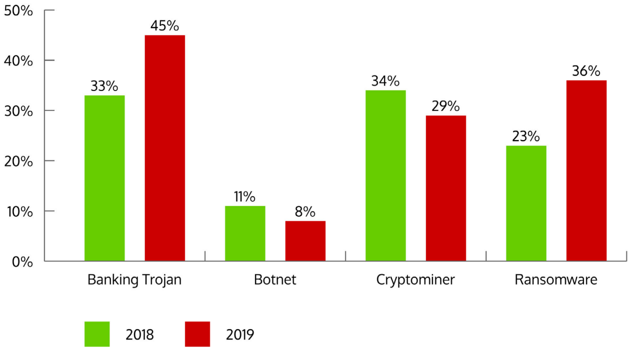


FIGURE 6. Percentage of new (previously unobserved) code by category [47].

III. AUTHENTICATION METHODS

This section contains an overview of elementary authentication primitives and their features. The defined primitives can be used to build any authentication scheme and are compatible with NIST Digital Identity Guidelines [45]. The main contribution of this section lies in the overview of the susceptibility of authentication methods to attacks from the presented taxonomy. Later we take a closer look at secure hardware because of its importance for concurrent e-banking authentication schemes.

The reader should gain a solid overview of authentication primitives whose knowledge is required for a proper understanding of the following section in which we discuss properties of multi-factor authentication and thus combinations of those primitives.

A. AUTHENTICATION PRIMITIVES

In this subsection, we describe the authentication primitives used for user verification in ICT systems. Every authentication scheme can be seen as a combination or specific use of those primitives. Nowadays, direct implementations of those primitives (methods) are not considered inherently secure and to achieve satisfiable security, modern authentication schemes combine multiple methods.

In Table 1, for eight identified authentication primitives, we observe four key characteristics (*replay*, *MITM* and *impersonation* resistances and *dynamic linking*). These characteristics were selected from requirements for authentication methods by NIST [45] based on their relevance to the e-banking area. *Replay resistance* is a fundamental feature preventing an adversary from recording the authentication process and replaying it at a later time, granting him unauthorised access. *Man-In-The-Middle resistance* prevents an adversary from positioning himself in the middle of the authentication process and manipulating the data flow. Under *impersonation resistance* we understand the verifiable identity of the authenticating user and non-repudiation of the authentication process. Lastly, we included *dynamic linking* as one of the key requirements of the PSD2 standard, which will be described later. It describes the ability to use this method to authenticate individual transactions (as opposed to authentication of the session).

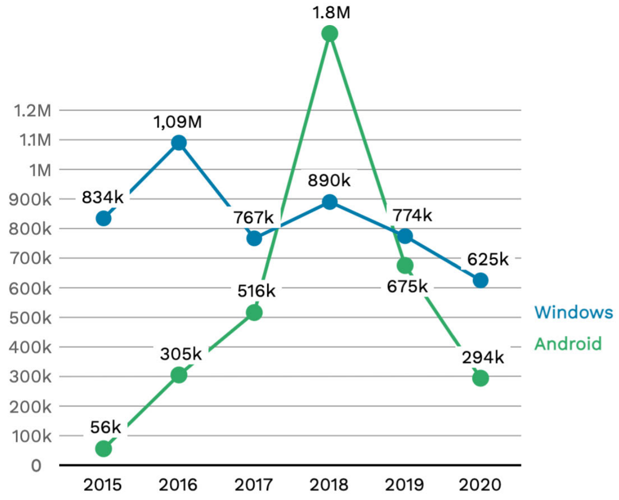


FIGURE 7. Users attacked by banking malware [54]–[58].

The classic approach is utilisation of basic *memorized secret* (**P-MSC**) such as static password or PIN code. Nowadays, we assume the usage of TLS for transport encryption, but despite this, the method shows the weakest resistance against various attacks and alternative authentication options are actively researched [64]. The resistance was greatly improved by facilitating some form of dynamic passwords, and their first usage was in the form of *look-up secrets* (**P-LUS**) represented by grid cards. A grid card contains a matrix of random combinations of alphanumeric characters, and the authentication is based on XY coordinate look-up system [65]. Because of the limited usability as the user was required to look up and construct the code himself, this primitive was practically replaced by HW tokens and SMS codes, where SMS codes are the most commonly used *out-of-band* method (**P-OOB**).

Similarly, the direct *cryptographic authentication* (**P-SCR** and **P-MCR**) based on public key infrastructure (PKI) never spread even though it has superior security features. Mostly because of the usability limits as it imposes the burden of managing private keys on the user. The difference between single-factor (**P-SCR**) and multi-factor (**P-MCR**) lies in the former one keeping the key on the device accessing the e-banking, while the latter keeps the key on a separate device, such as a smart card, which improves not only security but also usability as the key management is usually ensured by the device vendor. The implementations of P-MCR, which we find feasible in the near future, are payment cards, government ID cards, U2F authenticators, and cryptographic smart cards with asymmetric cryptography.

TABLE 1. Overview of authentication primitives and their features.

	Primitive	Replay Resistance	MITM Resistance	Impersonation Resistance	Dynamic Linking
P-MSC	Memorized secret	✗	✗	✗	✗
P-LUS	Look-up secret	✓	✗	✓	✗
P-SCR	Single-factor cryptographic authentication	✓	✓	✓	✓
P-MCR	Multi-factor cryptographic authentication	✓	✓	✓	✓
P-MFO	Multi-factor OTP device	✓	✓	✓	Opt.
P-OOB	Out-of-band authentication	✓	✗	✗	Opt.
P-SFO	Single-factor OTP device	✓	✓	✓	✓
P-BIO	Biometric authentication	✗	✗	✗	✗

Opt. (Optional) - depends on the implementation

The first dynamic password primitive that penetrated the market was *multi-factor OTP device* (**P-MFO**) consisting of various HW tokens generating one-time passwords (OTP). The first generation of those OTP devices was HW tokens with a display (often called "calculator") generating passwords that the user had to retype into e-banking. The following generations usually include some interface to ease the password transfer, such as USB or wireless connections (Bluetooth, NFC) or standard chip payment card interface (EMV). The EMV standard for the user and transaction authentication in e-banking is used in MasterCard as the Chip Authentication Program (CAP), while in VISA it is known as Dynamic Passcode Authentication (DPA) [66]. Some tokens lack the display, therefore the ability to show the details of an operation undergoing, and such tokens provide authentication based only on its presence.

The modern trend in OTPs is the usage of mobile applications as dynamic password generator (DPG). This approach simulates HW tokens in SW and often implements a challenge-response protocol. In case this DPG is run as a part of an e-banking application, we talk about a *single-factor OTP device* (**P-SFO**). Much more frequented is a case where this DPG is packed as a separate application, and if we accept that the mobile operating system securely isolates those applications, we can consider it a *multi-factor OTP* despite running on one device. A special case of a multi-factor OTP on one device is the utilisation of a secure enclave – a special cryptographic chip dedicated to key management and isolated from the rest of the system and thus even the e-banking application. We describe the secure enclave in detail in Section III-B.

With the spread of biometric sensors (such as fingerprint readers, face, voice and retina recognition) the inherent features of the user started to be used for authentication (**P-BIO**) as well. The biggest problem of biometrics is uncertainty as the biometrics compares the sensor data with a stored model and returns binary result – verified / unverified – depending on whether the comparison exceeds a given threshold. Because pure biometrics is not resistant against attacks such as replay or MITM, it is usually used bundled with secure key storage or as additional protection of other methods. The main issue of using biometrics as the primary authentication method is that biometric authentication gives local information about successful authentication, but it is difficult to transfer this information to the remote server securely. Existing attempts to achieve secure transfer (called crypto biometrics) are still not mature enough.

After we described the primitives, we take a deeper look at the feasibility of attacks described against selected most frequently used implementations of each authentication primitive (Table 2), which we call authentication methods. It turned out that the NIST requirements are not detailed enough for the assessment of authentication methods in the banking industry. Thus, we have to use more categories (linked to the attacks categories in Figure 3) to describe authentication mechanisms in full detail. It is essential to define the features of individual primitives as later in Section IV we discuss multi-factor authentication, and these features have a direct impact on compounds. If a method is resistant to an attack, then the multi-factor containing this method is resistant as well. E.g., a multi-factor scheme has replay resistance if at least one of the used factors has replay resistance.

In Table 2, we have examples of authentication methods (and their primitives) in the rows and selected attacks in the columns. The attack list is not complete because we omitted the irrelevant attacks (such as the whole category A–4 Attacks Focused on Banks) and merged attacks with the same features (such as Social Engineering based attacks).

We put the check mark if the attack is viable and cross mark for methods resistant to the attack. In case there are some constraints affecting the attack feasibility, we evaluated the most commonly used option and put the result in brackets.

B. SECURE HARDWARE AND ENCLAVE

Secure Hardware (also a trusted device) is a hardware module equipped with a microprocessor containing some security relevant data (keys) and algorithms for manipulating them (see Figure 8). This specialised hardware ensures both logical security by isolating such data from the system and hardware security as these modules are designed to be tamper-proof. The features of secure hardware can be utilised in several ways:

1) Storage of data, which can be manipulated only in a specific way (e.g., counter with only decrease operation allowed).
2) Storage of cryptographic private key allowing only selected operations such as encryption and never revealing the key itself.
3) Operating System integrity, where thanks to secure boot mechanism, secure hardware provides trust that the OS (and its security functions like process separation) hasn't been tampered with.

Ten years ago, in our previous article [1] we stated: "*Most widely use of the trusted device is a smart card. Smart cards offer very cheap implementation of one of the security concepts, and this concept is called tamper-resistant hardware.*" This statement is, obviously, not valid anymore. Nowadays, secure hardware is present in personal computers as Trusted Platform Module (TPM) chips and even in mobile devices as Apple Secure Enclave or Android Keystore System.

With respect to online services, FIDO (Fast IDentity Online) Alliance is the main driving force in the adoption of these technologies. Their protocol FIDO2 [67] consisting of W3C (World Wide Web Consortium) open web standard WebAuthn [68] and CTAP2 is becoming the de facto standard for using secure hardware for authentication in a web environment as it is implemented in all major browsers. While older FIDO standards enabled either local biometrics (FIDO UAF [69]) or Hardware Authentication Module (FIDO U2F [70]) to be used as a second factor for web services, FIDO2 includes support for both second factors and can even be used as a single authentication factor for passwordless authentication.

In general, the secure hardware can be implemented in multiple ways, where some lost the status over time:

Personal Computer (PC) In the infancy of information technology, PCs were considered a trusted device, which protects the interests of the user. The massive spread of malware and cyber-attacks destroyed this principle.

Smartcard Smartcard (electronic payment card or electronic ID card) appears to be an almost ideal implementation of secure hardware. It is cheap, security-hardened, provides cryptographic operations and is easy to manipulate. The main issue is the lack of a user interface requiring a special connector (either hardware or radio) to utilise its features. An example of current usage is CAP/DPA.

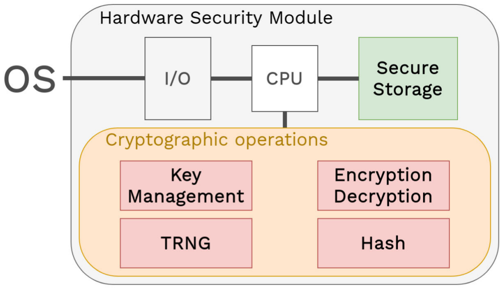


FIGURE 8. High level hardware security module architecture.

Cell phone Traditionally, the cell phone was used as a secure device by utilising the SIM card either through SIM Toolkit or SMS authentication. But SIM Toolkit is scarcely used because of the limitations of SIM card applications and SMS authentication does not comply with new PSD2 factor independence requirements and thus cannot be seen as the primary authentication mechanism in the future.

Hardware Authentication Token Traditionally, these devices take the form of an "authentication calculator". Despite the initial high price and lack of standardisation, they overcame the problems and became the widespread secure device. They declined in favour of SMS authentication but might see a comeback with a new generation featuring wired or wireless interfaces.

Hardware Security Module (HSM) HSM is a separate chip satisfying secure device requirements. It can be added to a system to bring secure device features such as key storage, cryptographic operations and true random number generator. In PCs, it is usually represented by TPM (although it serves mostly as the root of trust and does not offer full HSM possibilities), and in smartphones there are options like Apple Secure Enclave and Android Keystore System, which are discussed in the next subsection.

The modern addition to the secure devices is **Secure Enclave** which implements a trusted execution environment (TEE) concept, where an application is being run isolated from the operating system and protected from outside threats. A secure enclave guarantees confidentiality, integrity, and security for the application running within it [71]. TEE extends the concept of secure devices by allowing us to run arbitrary operations (opposed to a very specific set of operations in HSM) within the device while maintaining a high level of trust and security. Examples of secure enclave technology are Intel® SGX and ARM TrustZone.

1) SECURE HARDWARE IN SMARTPHONES

Because modern banking trends focus on smartphones and mobile banking, we describe the possibilities of smartphones

TABLE 2. Viable attacks on authentication methods.

	Password Guessing	Exhaustive Search	Social engineering (Phishing)	Pharming	Cross-channel attacks	Malware	AI Attacks	Physical credential stealing	Unauthorised Binding	Eavesdropping	Data manipulation	MITM
	A-1.1	A-1.2	A-1.3, A-1.6	A-1.4	A-1.5	A-1.7	A-1.8	A-2.1	A-2.2	A-3.1	A-3.2	A-3.3, A-3.4
Static password, PIN (P-MSC)	✓	✓	✓	✓	N/A	✓	✗	✗	(✓)[1]	(✓)[2]	✓	✓
Grid card (P-LUS)	✗	✓	✓	✓	N/A	✗	✗	✓	(✓)[1]	✗	✓	✓
Dynamic password generator (P-SFO)	✗	✗	✗	(✗)[3]	(✓)[4]	✓	✗	✓	✓	✗	(✗)[3]	(✗)[3]
PKI (P-SCR)	✗	✗	✗	✗	N/A	✓	✗	✗	✓	✗	✗	✗
PKI token (P-MCR)	✗	✗	✗	✗	N/A	✓	✗	✓	✓	✗	✗	✗
SMS Code (P-OOB)	✗	(✓)[5]	✗	✓	✓	✓	✗	✓	✓	✓	(✗)[3]	(✗)[3]
HW tokens with display (P-MFO)	✗	(✓)[5]	✗	(✗)[3]	N/A	✗	✗	✓	✓	✗	(✗)[3]	(✗)[3]
HW tokens without display (P-MFO)	✗	(✓)[5]	✗	✓	N/A	✓	✗	✓	✓	✗	(✗)[3]	(✗)[3]
Secure Enclave (P-MFO)	(✓)[6]	✓	✗	✗	N/A	✓	✗	✓	✓	✗	✗	✗
Biometric authentication (P-BIO)	✗	✗	✗	✓	N/A	✓	✓	✗	✓	(✓)[7]	✓	✓

[1] In case the user can reset the authentication method (password reset, resend grid card) the attack is possible.

[2] If there is no HSTS header set, an adversary might force unencrypted connection.

[3] The method is vulnerable in case that it does not support Dynamic Linking as defined in PSD2 directive.

[4] Applies only if the DPG is running on different device than e-banking (2da – see section IV-B).

[5] In case the length of the one-time cryptogram is not sufficient, and attempts are not limited.

[6] If the enclave is unlocked by a password, an attacker may use password guessing.

[7] Depends on the implementation parameters.

in detail. As we have mentioned in the previous section, SIM card use as a root of trust is becoming obsolete with SIM Toolkit long gone and SMS being replaced by other means, especially HSM seem to be a very promising candidate. Both major smartphone OS's include HSM support.

Apple Secure Enclave (ASE) is Apple's implementation of secure hardware, which (since the iPhone 5) is tightly integrated into iOS due to Apple developing both the iOS operating system and the iPhone hardware. It provides standard HSM features such as secure storage, random number generator and cryptographic operations (key generation, encryption/decryption, and hashing). ASE extends those features with person-to-device authentication using fingerprints, face image or password, as well as secure communication with corresponding sensors [72].

Android Keystore System (AKS) covers the secure hardware in the Android operating system from Google and, unlike ASE, is not bound to a specific HSM as different HW vendors include various modules [73]. Depending on the module provided, AKS supports different security assurance levels starting with *Secure Element*, which can only store cryptographic keys and is represented usually by SIM card or EMV chip. More advanced phones offer true HSM chips not only for key storage but they also include cryptographic operations and random number generators. The most advanced approach offers full TEE able to run custom applications in a secure environment independent from the OS.

IV. MULTI-FACTOR AUTHENTICATION

Multi-factor authentication is a common technique to increase the strength of the authentication process by combining multiple factors (methods). The resulting scheme inherits their properties (such as resilience to specific types of attacks). The usual perception of these combinations must be revised for the e-banking sector due to the new European directives, which bring additional requirements. Thus, some common combinations cease to be viable. The main contribution of this section is our classification of authentication schemes, which is compatible with both the NIST Digital Identity Guidelines [45] and the EU PSD2 regulations [9].

A. PSD2 DIRECTIVE MOTIVATION

The security of authentication in internet banking applications is being pushed forward also by EU activities. The big step came on September 14th, 2019, when the Regulatory Technical Standards (RTS) of the Revised Payment Service Directive (PSD2) started to be mandatory for the EU banks [74]. The end of the migration period for PSD2 Strong Customer Authentication is December 31th, 2020, but every country can temporarily mitigate the effects by delaying the enforcement.

The concepts enforced by PSD2 to the area of client authentication are *two factor authentication* (with requested *factor independence*), *strong customer authentication* (SCA) and the *dynamic linking* of the authentication code to the transaction's beneficiary and amount. The next requirement is *cloning protection* – the ability to withstand memory cloning attacks.

For the sake of completeness, it should be added that as far as regulatory technical standards for strong client authentication and common and secure open communication standards are concerned, PSD2 is further complemented by Commission Delegated Regulation (EU) 2018/389 [75]. In addition to security requirements, it specifies further technical details such as auditability requirements, technology neutrality in the implementation of authentication codes, interface quality requirements, the use of open standards, but also defines exceptions to strong authentication. The exceptions are usually determined by the type of transaction and the presence of additional risk mitigation measures such as low-value contactless payments at the point of sale, which also take into account the maximum number of consecutive transactions.

From our point of view, the two main PSD2 requirements are the factor independence and SCA that together form the requirements for multi-factor authentication (covered later in this section). But it is necessary to say that the SCA requirement is stronger than the general requirement for multi-factor authentication because SCA requires at least two methods from the exact list of primitive categories and not an arbitrary combination of methods. Cloning protection is an additional security requirement, and dynamic linking only allows usage for other purposes than pure authentication.

1) STRONG CUSTOMER AUTHENTICATION (SCA)

The term Strong Customer Authentication is defined in the document *Directive (EU) 2015/2366 of the European Parliament and of the Council* [9]. The definition in *Article 4 – Definitions* paragraph 30 states: "*"strong customer authentication" means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.*"

2) FACTOR INDEPENDENCE

Furthermore, *Article 9 - Independence of the elements* of *Commission Delegated Regulation (EU) 2018/389* [75] supplementing the same regulation defines that:

1. *Payment service providers shall ensure that the use of the elements of strong customer authentication referred to in Articles 6, 7 and 8 is subject to measures which ensure that, in terms of technology, algorithms and parameters, the breach of one of the elements does not compromise the reliability of the other elements.*
2. *Payment service providers shall adopt security measures, where any of the elements of strong customer authentication or the authentication code itself is used through a multi-purpose device, to mitigate the risk which would result from that multi-purpose device being compromised.*

3. *For the purposes of paragraph 2, the mitigating measures shall include each of the following:*
   (a) *the use of separated secure execution environments through the software installed inside the multi-purpose device;*
   (b) *mechanisms to ensure that the software or device has not been altered by the payer or by a third party;*
   (c) *where alterations have taken place, mechanisms to mitigate the consequences thereof.*

3) CLONING PROTECTION

The additional requirements for authentication defined in Article 7 - *Requirements of the elements categorised as possession* of the same supplement are particularly relevant for mobile devices. This article says that " *The use by the payer of those elements shall be subject to measures designed to prevent replication of the elements.* [75]"

4) DYNAMIC LINKING

The term dynamic linking is defined in Article 5 of the supplement as well, and it states that payment transaction details should be protected and tied to authentication:

1. *Where payment service providers apply strong customer authentication in accordance with Article 97(2) of Directive (EU) 2015/2366, in addition to the requirements of Article 4 of this Regulation, they shall also adopt security measures that meet each of the following requirements:*
   (a) *the payer is made aware of the amount of the payment transaction and of the payee;*
   (b) *the authentication code generated is specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction;*
   (c) *the authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and to the identity of the payee agreed to by the payer;*
   (d) *any change to the amount or the payee results in the invalidation of the authentication code generated.*

The PSD2 requirements for Strong Customer Authentication and Factor independence make an urgent demand for the new group of authentication mechanisms called multi-factor authentication mechanisms. Thus, in the following section, we will prospect viable combinations of authentication methods and how these combinations (called authentication schemes) will meet the PSD2 requirements.

B. MULTI-FACTOR ASSESSMENT

In Table 3, we describe features of common combinations of authentication methods. The reader's main takeaway is the quick overview of the possibilities and their features with respect to the PSD2 requirements, which we consider the most advanced in the e-banking area. The table uses the same notation as previous tables, where checkmark denotes that the combination of methods satisfies the requirement and cross mark that it doesn't. If the mark is in brackets, the assessment is not unambiguous, in which case we used the more common rating and added the condition in the footnote. In case the feature can be enabled possible by some additional adjustment of the basic scheme, we use 'Opt.' as in the optional feature.

For further ease of understanding, we state the category of the given scheme as defined by Frederik Mennes in his SCA requirement analysis [76]. There are four categories based on the segregation of the factors:

1aa (one-app-authentication) describes the e-banking apps with built-in authenticators

2aa (two-app-authentication) means both authentication and e-banking apps are separate apps

2da (two-device-authentication) extracts authentication to a separate device

oob (out-of-band) uses a third party (such as telco service) for authentication

C. TRENDS IN MULTI-FACTOR AUTHENTICATION

What we consider interesting is the continuous evolution of a typical e-banking system, especially in the authentication and authorisation area. It moved from *password-based* authentication, over HW tokens and SMS codes, to currently used *Dynamic passwords* generated by mobile applications.

We can essentially divide authentication schemes into four categories based on their viability. The first category, we call it *Schemes on retreat*, contains an ever-growing group of deprecated schemes used from the beginning of the e-banking era. The schemes that declined in use but with some adaptation or under special conditions can be used again belong to the second category - *Reincarnating schemes*. Then, described in *Schemes still here with us*, we have a group of robust schemes which keep their properties over the span of time. The last category contains the schemes based on novel approaches, which are emerging in the e-banking area, and we call them *Schemes on the rise*.

1) SCHEMES ON RETREAT

The classic method used in early authentication schemes was *password* authentication. Because of the lack of resistance against phishing and replay attacks, it was soon replaced. The combination with *PIN* did not bring much improvement as both are static, memorable secrets, but the combination with *Grid cards* brings replay resistance and force the adversary to recover (usually by phishing) a substantial part of the grid card in order to perform an attack.

Later the usage of *SMS codes* used telecommunication services for OTP delivery, which improved usability and shifted the security from banks to the telco providers (attacks such as SIM Swapping and SS7 attacks became relevant). The decline of this scheme was brought by the spread of mobile banking and the factor independence requirement of PSD2. If the user

TABLE 3. PSD2 features of authentication methods and their combinations.

Method combination	Cloning protection	Factor independence	Dynamic linking	SCA	Comment
Password	✗	✗	✗	✗	
Password + PIN	✗	✗	✗	✗	
Password + Grid card	✗	✓	✗	(✓)[1]	2da
PKI (private key) protected by password	✓	✗	✓	✗	
HW Token (MCR)	✓	✓	✓	✓	2da
HW Token protected by PIN	✓	✓	✓	✓	2da
HW Token protected by BIO	✓	✓	✓	✓	2da
SMS	(✓)[2]	✗	Opt.	✗	oob
Password + SMS	(✓)[2]	✓	Opt.	(✓)[3]	oob
Integrated DPG protected by password (SFO)	(✗)[4]	(✗)[5]	✓	(✗)[5]	1aa
Separated DPG protected by password (MFO)	(✗)[4]	(✓)[4]	✓	(✓)[4]	2aa
Dynamic password + BIO	(✗)[4]	✓	✓	(✓)[4]	2aa
BIO	✗	✗	✗	✗	
BIO + Password	✗	✓	✗	✓	
BIO + SMS	(✓)[2]	✓	Opt.	✓	oob
PKI (private key) protected by BIO	(✗)[4]	✗	✓	✗	
Secure Enclave protected by BIO	✓	✓	✓	✓	
Secure Enclave protected by password	✓	✓	✓	✓	

[1] Technically could be considered valid, but in reality is not used as such.
[2] Indirectly possible by attacks on telecommunication links such as SIM Swapping and SS7 attacks.
[3] To fulfil SCA requirements, the SMS receiving device have to be independent of the other one where the password is entered. Nowadays, this is difficult to achieve.
[4] Depends on OS capabilities, in case of rooted OS (called jailbreak in iOS) cannot be ensured [78]. E.g. biometrics is cloneable by design, and protection depends on second factor properties.
[5] The satisfiability of factor independence is not decided yet; if it does not satisfy factor independence, it isn't SCA.

receives the SMS code on the same device where the mobile banking is running, the malware can compromise both at once, breaking the requirement.

These schemes by themselves cannot satisfy the SCA requirements, but methods used in these schemes can be combined to create more resilient schemes. Such an example is the combination of SMS with a password which would comply with the SCA.

2) REINCARNATING SCHEMES

A few years ago, the *Hardware Tokens* were the most spread method for authentication. They represent the first true OTP systems, and as every code is unique and generated by a specially crafted single-purpose device, it provides very high security. The tokens started declining because of the usability constraints as they required users to carry an extra device and manually transfer the generated code into the e-banking system. Despite the fact that they were superseded by *SMS codes*, the situation changes because, unlike SMS, they easily satisfy the SCA requirements of PSD2, and the burden of manual code transfer is overcome by the new generation of HW Tokens with NFC/Bluetooth technologies. Furthermore, the HW tokens are usually protected by passwords or biometrics, which mitigate the risk of theft.

3) SCHEMES STILL HERE WITH US

The schemes based on *PKI* method use the full power of modern cryptography directly, which make them very resilient. The attempts of using those schemes have been present since the beginning of e-banking, but overhead and lack of usability for a common user prevented their spread. Nevertheless, the PKI found its use in HW Tokens and smart cards. The private key is usually further protected by encryption and some other factors such as passwords or biometrics.

The schemes based on PKI can be SCA compliant, but they are strongly dependent on the usage because if used incorrectly, they do not satisfy the factor independence.

4) SCHEMES ON THE RISE

The advances in technology enabled new methods to emerge. The most apparent is the spread of *Biometrics* for authentication, which prevailed mostly in smartphones despite the fact that standalone biometrics is not mature enough yet and can thus be used only in combination with another method. The common use of biometrics is strengthening the KYC process for remote customer verification or device authorisation when using a hardware token, a dynamic password generator or secure enclave.

Secure Enclave is a relatively recent addition to the authentication methods, which was briefly covered in Section III-B. A secure enclave is usually protected by other authentication methods (password, PIN or biometrics) and, apart from providing key storage and cryptographic operations, is used as a root of trust and checks the integrity of operating systems and applications. These integrity features are used to defend the factor independence of standalone e-banking and authentication apps.

The typical e-banking system nowadays utilises a mobile application generating *Dynamic passwords*, which is usually protected by either user *password* or *biometrics* if the smartphone supports it. In case this application is distinct from the mobile banking application, and we trust the mobile operating system to isolate contexts of different applications properly, this approach satisfies factor independence condition and is thus preferred by EU banks.

FIDO2 is the concurrent standard for including biometrics and hardware tokens for online authentication. However, despite its spread in fintech and other web services, the adoption in e-banking is still in its infancy. Examples of banks already including it are Bank of America[1] (member of FIDO Alliance) or Boursorama Banque.[2]

5) ADDITIONAL CLARIFICATION

In our work, we have described only two-factor combinations and not the general multi-factor. We decided to narrow this area for the sake of clarity and because multiple factors are usually used chained, where one factor is strengthened by another such as HW Token as a second factor further protected by a PIN. Furthermore, multi-factor combinations of third and higher order usually do not satisfy the factor independence, and their security features require deeper analysis.

The class *Integrated DPG protected by password* is the subject of research and discussions as it is unclear whether a DPG included within mobile banking application satisfies the SCA requirements [77]. To be considered SCA compliant, such an application has to meet multiple conditions such as *secure device boot*, *secure checking of application integrity* to ensure the application hasn't been tampered with and strong protection against attacks from other applications. In the now prevalent mobile environment, it is usually required that the device is not rooted (or jailbroken), which would allow full access to all application contents breaking cloning protection and factor independence at once. The solution for the future is protecting the application against attacks from the operating system by utilising secure hardware.

D. BROADER PERSPECTIVE

Our primary focus is on authentication methods and schemes. However, there are many other methods to increase security or, specifically in the e-banking area, to reduce the risk of fraud. The output of these methods is usually a score representing the level of the risk (which can be calculated by combining multiple sources), so we consider them as risk management tools. However, they cannot be used for authentication on their own, nor in combination with another factor. One of the used principles is continuous authentication, which constantly monitors selected parameters. For example, it can enhance biometric authentication by continuous sample evaluation (face is constantly scanned by a camera) or analyse behavioural metrics such as user behavioural patterns (e.g. payer/payee location, spending habits). In some cases (such as low-risk transactions), an appropriate combination of score sources could be sufficient to replace SCA in e-banking [75].

In a wider context, with the standardisation of authentication requirements under PSD2, the focus shifts on setting up and consolidating e-identity (eID) systems because they are seen as an important element of future payment systems. It remains an open question what role banks should play within these systems. In Europe, two different approaches can

[1] https://www.bankofamerica.com/security-center/online-mobile-banking-privacy/usb-security-key/

[2] https://www.boursorama.com/aide-en-ligne/mon-espace-client/identifiant-et-mot-de-passe/question/en-quoi-consiste-la-connexion-par-cle-de-securite-sur-internet-5165516

be distinguished – bank-driven eID, where banks are identity providers (e.g. Norway, Sweden or the Czech Republic), and government-driven eID, where banks are mere consumers (e.g. Belgium and Estonia) [78]. Given the potential consolidation of eIDs, PSD2 SCA requirements (as well as other requirements) may impact other e-services, so a thorough evaluation of authentication methods will have wider implications.

V. RELATED WORK

While there are many manuscripts dealing with e-banking security, they usually either broadly cover the topic for business executives [10], [79], focus on a narrow area (e.g. specific types of systems [11], malware [12], [14], usability [80]) or they are location specific (e.g. Switzerland [2], Brazil [3], India [81], Nigeria [82]). On the other hand, in the area of authentication, most of the literature cover general problems [83]–[85]. This fragmentation makes it difficult to develop a coherent view of the current state of the art.

We have also found that a number of papers are outdated and need to be revised to take into account new approaches and regulations such as PSD2.

In related work, we focus on two main areas: attack taxonomies and authentication methods used in e-banking. We also add a third area where we briefly mention usability aspects.

A. ATTACK TAXONOMY

Many works have addressed the classification of attacks in the online environment. There are general overviews, such as Authenticator Threat/Attack from NIST [45], but more common are more narrowly focused taxonomies. Examples of such could be Android financial malware attack taxonomy by Kadir *et al.* [15], banking trojans taxonomy by Kiwia *et al.* [13], or phishing attacks classification by Gupta *et al.* [86].

In our work, we introduce a high-level attack taxonomy tailored specifically for e-banking (as opposed to NIST) while covering the entire domain. We believe that this taxonomy will provide a better understanding of the problem and will comprehensively link existing narrowly focused classifications in the e-banking domain.

B. AUTHENTICATION METHODS IN E-BANKING

The available research in authentication methods in e-banking lately consists of analysing solutions deployed by selected banks and their features. We can see the great variability of the area as virtually every bank develops its authentication solutions independently.

Chaimaa *et al.* [87] recently published an overview of e-banking services, summarising the available research, based mostly on outdated papers (5 years old and more). The grasp of this article is very superficial, while in contrast, our article provides a more comprehensive and deeper insight.

Kiljan *et al.* conducted a survey about the usage of authentication schemes in online banking [88] by actively researching 80 banks across the world. They found that most banks use passwords for single-factor authentication, while PIN is used in multi-factor schemes. SMS has gained popularity, but they already argue about the security of connected (online) possession factors. They mention behaviour anomaly detection as a form of biometrics, but as this factor is fully implemented in the backend, they have not been able to verify its use. The conclusion is that the adoption of multi-factor authentication has increased in all regions except North America and that authentication and transaction authorisation need to be unified across the banking area.

One of the main works in the e-banking authentication area is a survey published by Sinigaglia *et al.* [89], which reviews the EU regulations and strong authentication mechanism implemented by 26 major EU and non-EU banks for their online payment systems. The analysis is based on available public bank documentation. One of their key findings is a diversity of implementations which opens a large attack surface and observation that mobile devices became privileged targets and single point of failure.

Sinigaglia *et al.* further extend their work with a stronger focus on multi-factor authentication [90] while distinguishing between the internet and mobile payments. Again they took a sample of EU and non-EU banks and evaluated their multi-factor authentication with respect to the existing regulations and best practices, security, and complexity. They conduct a comparison of available documents in terms of requirements and analyse the applicability of seven attacker models to identified authenticators. For all included banks, they describe an overview of deployed authentication protocols, their compliance, susceptibility to attacks, and complexity.

In comparison with our work, due to frequent changes, we neglect specific technical solutions and focus on general authentication principles and their compliance with regulations. Additionally, we also propose a complex e-banking attack taxonomy and a more detailed analysis of authentications mechanisms vulnerabilities.

C. USABILITY

The usability of authentication methods and other e-banking solutions is an important parameter for user adoption. Although we do not address this topic in our paper, we consider it important for a comprehensive understanding of the context. We selected two papers to demonstrate the acceptability of more complex multi-factor authentication solutions by the public.

MFA authentication has become more accepted by users, as shown, for example, by Althobaiti and Mayhew [91]. They conducted a survey among 302 e-banking users and concluded that users feel confident using tokens, which they perceive as more secure.

Lyastani *et al.* [92] show that FIDO has a great potential for web user authentication due to its high usability, which users consider more acceptable than password-based authentication.

VI. CONCLUSION

In the paper, we cover the state of the current e-banking authentication area to enable the reader to have an easy orientation in the problem. The existing materials usually cover the general authentication mechanisms and do not focus on the e-banking specifics, or, on the other hand, are too specific and detailed to provide a comprehensive overview. Our paper suggests a taxonomy for attacks on e-banking compatible with general authentication taxonomy by NIST [45] and a comprehensive overview of authentication schemes and their resistance against those attack classes.

Because the *Payment Services Directive 2 (PSD2)* by European Union brings important security requirements for the banking area, which we find the most advanced in the world, we discuss security features of authentication schemes in the context of this standard. For every scheme, we discuss the satisfaction of Strong Customer Authentication (SCA) as well as other essential features as described in PSD2.

Moreover, we provide the reader with an informed discussion about trends in multi-factor authentication schemes and conveniently group them into four classes depending on their current usage and future prospects. We point out unresolved issues, especially in the area of the feasibility of mobile devices as a secure element.

The main contribution of the article is a comprehensive overview of authentication schemes and their security evaluation. We emphasize viable combinations of authentication methods concerning the concurrent standards, mainly PSD2.

REFERENCES

[1] P. Hanacek, K. Malinka, and J. Schafer, "E-banking security—A comparative study," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 25, no. 1, pp. 29–34, Jan. 2010.

[2] Swiss Finance Council. (2020). *Getting Ready for the '20s-Technology and the Future of Global Banking*. Accessed: Feb. 15, 2021. [Online]. Available: https://www.swissfinancecouncil.org/images/SFC_Discussion_Paper_2020.pdf

[3] Deloitte. (Aug. 2020). *FEBRABAN Banking Technology Survey*. Accessed: Jan. 20, 2021. [Online]. Available: https: //www2.deloitte.com/content/dam/Deloitte/br/Documents/financial-services/2020%20FEBRABAN%20Banking%20Technology%20Survey.pdf

[4] Deloitte. (2019). *Global Mobile Consumer Survey: UK Cut*. Accessed: Feb. 15, 2021. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/technology-media-telecommunications/deloitte-uk-plateauing-at-the-peak-the-state-of-the-smartphone.pdf

[5] Pew Research Center. (Feb. 2019). *Smartphone Ownership is Growing Rapidly Around the World, but Not Always Equally*. Accessed: Feb. 15, 2021. [Online]. Available: https://www.pewresearch.org/global/wp-content/uploads/sites/2/2019/02/Pew-Research-Center_Global-Technology-Use-2018_2019-02-05.pdf

[6] EY. (2019). *Global FinTech Adoption Index 2019*. Accessed: Feb. 15, 2021. [Online]. Available: https://assets.ey.com/content/dam/ey-sites/eycom/en_gl/topics/financial-services/ey-global-fintech-adoption-index-2019.pdf

[7] EMVCo. (Sep. 2021). *EMV 3-D Secure Protocol and Core Functions Specification*. Accessed: Dec. 6, 2021. [Online]. Available: https://www.emvco.com/emv-technologies/3d-secure/

[8] Security Standards Council. (May 2018). *Payment Card Industry (PCI) Data Security Standard*. Accessed: Nov. 27, 2020. [Online]. Available: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

[9] E. Union, "Directive (EU) 2015/2366 of the European parliament and of the council," *Off. J. Eur. Union*, vol. 337, pp. 35–127, Nov. 2015.

[10] L. Pascu. (2018). *Top Security Challenges for the Financial Services Industry in 2018*. Bitdefender. Accessed: Feb. 15, 2021. [Online]. Available: https://www.bitdefender.com/files/News/CaseStudies/study/240/Bitdefender-Top-Security-Challenges-for-the-Financial-Whitepaper-EN-interactive.pdf

[11] F-Secure. *Threat Analysis: SWIFT Systems and the SWIFT Customer Security Program*. Accessed: Nov. 13, 2020. [Online]. Available: https://www.f-secure.com/content/dam/f-secure/en/business/common/collaterals/f-secure-threat-analysis-swift.pdf

[12] M. A. Kazi, S. Woodhead, and D. Gan, "A contemporary taxonomy of banking malware," in *Proc. Int. Conf. Sci. Comput. Cryptogr.*, Dec. 2018, p. 7. [Online]. Available: https://www.researchgate.net/publication/344017237_A_Contempory_Taxonomy_of_Banking_Malware

[13] D. Kiwia, A. Dehghantanha, K.-K.-R. Choo, and J. Slaughter, "A cyber kill chain based taxonomy of banking Trojans for evolutionary computational intelligence," *J. Comput. Sci.*, vol. 27, pp. 394–409, Jul. 2018.

[14] P. Black, I. Gondal, and R. Layton, "A survey of similarities in banking malware behaviours," *Comput. Secur.*, vol. 77, pp. 756–772, Aug. 2018.

[15] A. F. A. Kadir, N. Stakhanova, and A. A. Ghorbani, "Understanding Android financial malware attacks: Taxonomy, characterization, and challenges," *J. Cyber Secur. Mobility*, vol. 7, no. 3, pp. 1–52, Jul. 2018.

[16] W. Melicher, B. Ur, S. M. Segreti, S. Komanduri, L. Bauer, N. Christin, and L. F. Cranor, "Fast, lean, and accurate: Modeling password guessability using neural networks," in *Proc. 25th USENIX Conf. Secur. Symp.* Berkeley, CA, USA: USENIX Association, 2016, pp. 175–191.

[17] R Hranický, L Zobal, O Ryšavý, and D Kolár, "Distributed password cracking with BOINC and hashcat," *Digit. Invest.*, vol. 30, pp. 161–172, Sep. 2019.

[18] K. D. Nguyen, H. Rosoff, and R. S. John, "Valuing information security from a phishing attack," *J. Cybersecur.*, vol. 3, no. 3, pp. 159–171, Nov. 2017.

[19] G. Ollmann. (Jul. 2005). *The Pharming Guide*. Whitepaper. Accessed: Feb. 15, 2021. [Online]. Available: https://research.nccgroup.com/wp-content/uploads/2020/07/thepharmingguide.pdf

[20] C. Karlof, U. Shankar, J. D. Tygar, and D. Wagner, "Dynamic pharming attacks and locked same-origin policies for web browsers," in *Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS)*. New York, NY, USA: ACM, 2007, pp. 58–71.

[21] K. Thomas, F. Li, A. Zand, J. Barrett, J. Ranieri, L. Invernizzi, Y. Markov, O. Comanescu, V. Eranti, A. Moscicki, D. Margolis, V. Paxson, and E. Bursztein, "Data breaches, phishing, or malware? Understanding the risks of stolen credentials," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.* New York, NY, USA: ACM, Oct. 2017, pp. 1421–1434.

[22] I. J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial nets," in *Proc. 27th Int. Conf. Neural Inf. Process. Syst. (NIPS)*, vol. 2. Cambridge, MA, USA: MIT Press, 2014, pp. 2672–2680.

[23] J. E. Tapia and C. Arellano, "Soft-biometrics encoding conditional GAN for synthesis of NIR periocular images," *Future Gener. Comput. Syst.*, vol. 97, pp. 503–511, Aug. 2019.

[24] K. Lee, B. Kaiser, J. Mayer, and A. Narayanan, "An empirical study of wireless carrier authentication for SIM swaps," in *Proc. 16th Symp. Usable Privacy Secur.* Berkeley, CA, USA: USENIX Association, Aug. 2020, pp. 61–79.

[25] K. Ullah, I. Rashid, H. Afzal, M. M. W. Iqbal, Y. A. Bangash, and H. Abbas, "SS7 vulnerabilities—A survey and implementation of machine learning vs rule based filtering for detection of SS7 network attacks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1337–1371, 2nd Quart., 2020.

[26] W. Yang, Z. Zheng, G. Chen, Y. Tang, and X. Wang, "Security analysis of a distributed networked system under eavesdropping attacks," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 7, pp. 1254–1258, Jul. 2020.

[27] E. Cronin, M. Sherr, and M. A. Blaze, "On the reliability of current generation network eavesdropping tools," *Int. Fed. Inf. Process.*, vol. 222, pp. 199–214, Jan. 2006.

[28] Y. Zeng and R. Zhang, "Wireless information surveillance via proactive eavesdropping with spoofing relay," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1449–1461, Dec. 2016.

[29] D. Li, H. Zhou, and W. Yang, "Privacy-preserving consensus over a distributed network against eavesdropping attacks," *Electronics*, vol. 8, no. 9, p. 966, Aug. 2019.

[30] J. Fuller, B. Ramsey, J. Pecarina, and M. Rice, "Wireless intrusion detection of covert channel attacks in ITU-T G.9959-based networks," in *Proc. 11th Int. Conf. Cyber Warfare Secur. (ICCWS)*, 2016, pp. 137–145.

[31] Tetra Defense. (Jan. 2019). *Data Manipulation: A Rising Trend in Cyberattacks, and How to Address it*. Accessed: Dec. 3, 2020. [Online]. Available: https://www.tetradefense.com/incident-response-services/data-manipulation-a-rising-trend-in-cyberattacks-and-how-to-address-it/

[32] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system," in *Proc. IEEE PES Gen. Meeting*, Jul. 2010, pp. 1–6.

[33] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2027–2051, 3rd Quart., 2016.

[34] M. Knežević, S. Tomović, and M. J. Mihaljević, "Man-in-the-middle attack against certain authentication protocols revisited: Insights into the approach and performances re-evaluation," *Electronics*, vol. 9, no. 8, p. 1296, Aug. 2020.

[35] F. Callegati, W. Cerroni, and M. Ramilli, "Man-in-the-middle attack to the HTTPS protocol," *IEEE Secur. Privacy*, vol. 7, no. 1, pp. 78–81, Jan./Feb. 2009.

[36] The OWASP® Foundation. (2006). *Man-in-the-Browser Attack*. Accessed: Nov. 24, 2020. [Online]. Available: https://owasp.org/www-community/attacks/Man-in-the-browser_attack

[37] J. Petters. (Sep. 2020). *What is an Insider Threat? Definition and Examples*. Accessed: Nov. 12, 2020. [Online]. Available: https://www.varonis.com/blog/insider-threats/

[38] J. A. Hill, "SWIFT bank heists and article 4A," *J. Consum. Commercial Law*, vol. 22, no. 1, pp. 1–7, 2018.

[39] R. Cohen and D. Walkowski. (Aug. 2019). *Banking Trojans: A Reference Guide to the Malware Family Tree*. Accessed: Oct. 20, 2020. [Online]. Available: https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree

[40] A. Mauraya, N. Kumar, A. Agrawal, and R. Khan, "Ransomware: Evolution, target and safety measures," *Int. J. Comput. Sci. Eng.*, vol. 6, no. 1, pp. 80–85, 2017.

[41] The OWASP® Foundation. (2017). *OWASP Top Ten*. Accessed: Nov. 25, 2020. [Online]. Available: https://owasp.org/www-project-top-ten/2017/

[42] D. Watson, "Web application attacks," *Netw. Secur.*, vol. 2007, no. 10, pp. 10–14, Oct. 2007.

[43] Kaspersky. (2017). *What is a DDoS Attack?-DDoS Meaning*. Accessed: Nov. 9, 2020. [Online]. Available: https://www.kaspersky.com/resource-center/threats/ddos-attacks

[44] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques," *Int. J. Distrib. Sensor Netw.*, vol. 13, no. 12, Dec. 2017, Art. no. 155014771774146.

[45] P. A. Grassi, E. M. Newton, R. Perlner, A. Regenscheid, J. Fenton, W. Burr, J. Richer, N. Lefkovitz, J. Danker, Y.-Y. Choong, K. Greene, and M. Theofanos, "Digital identity guidelines: Authentication and lifecycle management," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST Special Publication, Tech. Rep., 800-63B, Jun. 2017.

[46] Organization of American States. (Sep. 2018). *State of Cybersecurity in the Banking Sectorin Latin America and the Caribbean*. Accessed: Feb. 15, 2021. [Online]. Available: http://www.oas.org/es/sms/cicte/sectorbancarioeng.pdf

[47] IBM. (2020). *IBM X-Force Threat Intelligence Index*. Accessed: Feb. 15, 2021. [Online]. Available: https://www.ibm.com/account/reg/signup?formid=urx-42703

[48] Accenture. (2019). *Future Cyber Threats*. Accessed: Feb. 15, 2021. [Online]. Available: https://www.accenture.com/_acnmedia/pdf-100/accenture_fs_threat-report_approved.pdf

[49] Accenture. (2018). *Phishing as a Service: The Phishing Landscape*. Accessed: Feb. 15, 2021. [Online]. Available: https://www.accenture.com/t00010101T000000Z_w_/gb-en/_acnmedia/PDF-71/Accenture-Phishing-As-Service.pdf

[50] E. Mikalauskas. (Sep. 2020). *Report: Buying Your Own Malware has Never Been Easier*. Accessed: Feb. 15, 2021. [Online]. Available: https://cybernews.com/security/buying-your-own-malware-has-never-been-easier/

[51] H. Poston. (2020). *Cybercrime at Scale: Dissecting a Dark Web Phishing Kit*. Infosec. Accessed: Feb. 15, 2021. [Online]. Available: https://resources.infosecinstitute.com/cybercrime-at-scale-dissecting-adark-web-phishing-kit/

[52] A. Lakhani. (Jul. 2020). *How Threat Researchers Leverage the Darknet to Stay Ahead of Cyber Threats*. Fortinet. Accessed: Feb. 15, 2021. [Online]. Available: https://www.fortinet.com/blog/threat-research/howthreat-researchers-leverage-darknet-to-stay-ahead-of-cyber-threats

[53] Accenture. (2019). *Know Your Threat: AI is the New Attack Surface*. Accessed: Feb. 15, 2021. [Online]. Available: https://www.accenture.com/_acnmedia/Accenture/Redesign-Assets/DotCom/Documents/Global/1/Accenture-Trustworthy-AI-POV-Updated.pdf

[54] Kaspersky. (Feb. 2017). *Financial Cyberthreats in 2016*. Accessed: Sep. 8, 2020. [Online]. Available: https://securelist.com/financial-cyberthreats-in-2016/

[55] Kaspersky. (Feb. 2018). *Financial Cyberthreats in 2017*. Accessed: Sep. 8, 2020. [Online]. Available: https://securelist.com/financial-cyberthreats-in-2017/

[56] Kaspersky. (Mar. 2019). *Financial Cyberthreats in 2018*. Accessed: Sep. 8, 2020. [Online]. Available: https://securelist.com/financial-cyberthreats-in-2018/

[57] Kaspersky. (Apr. 2020). *Financial Cyberthreats in 2019*. Accessed: Sep. 8, 2020. [Online]. Available: https://securelist.com/financial-cyberthreats-in-2019/

[58] Kaspersky. (Mar. 2021). *Financial Cyberthreats in 2020*. Accessed: Jan. 5, 2021. [Online]. Available: https://securelist.com/financial-cyberthreats-in-2020/

[59] Z. Bederna and T. Szadeczky, "Cyber espionage through Botnets," *Secur. J.*, vol. 33,s pp. 43–62, Sep. 2019.

[60] A. R. A. Grégio, V. M. Afonso, D. S. F. Filho, P. L. D. Geus, and M. Jino, "Toward a taxonomy of malware behaviors," *Comput. J.*, vol. 58, no. 10, pp. 2758–2777, Oct. 2015.

[61] A. Qamar, A. Karim, and V. Chang, "Mobile malware attacks: Review, taxonomy & future directions," *Future Gener. Comput. Syst.*, vol. 97, pp. 887–909, Aug. 2019.

[62] Kaspersky. (Jul. 2020). *Mobile Security: Android vs iOS-Which One is safer?*. Accessed: Feb. 15, 2021. [Online]. Available: https://www.kaspersky.com/resource-center/threats/android-vs-iphone-mobile-security

[63] D. Morán. (Oct. 2019). *Analyzing the Risk of Banking Malware in Android vs. iOS*. Accessed: Feb. 15, 2021. [Online]. Available: https://www.buguroo.com/en/labs/analyzing-the-risk-of-banking-malware-in-android-vs-ios

[64] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *Proc. IEEE Symp. Secur. Privacy*, May 2012, pp. 553–567.

[65] B. B. Balilo, Jr., B. D. Gerardo, and R. P. Medina, "A comparative analysis and review of OTP grid authentication scheme: Development of new scheme," *Int. J. Sci. Res. Publications*, vol. 7, no. 11, pp. 1–5, 2017.

[66] J. van den Breekel, D. A. Ortiz-Yepes, E. Poll, and J. de Ruiter, "EMV in a nutshell," Radboud Univ. Nijmegen, Nijmegen, The Netherlands, Tech. Rep., 2016. [Online]. Available: http://www.cs.ru.nl/~erikpoll/publications/EMVtechreport.pdf

[67] FIDO Alliance. (2019). *FIDO2: WebAuthn & CTAP*. Accessed: Nov. 26, 2021. [Online]. Available: https://fidoalliance.org/fido2/

[68] World Wide Web Consortium. (2021). *Web Authentication: An API for Accessing Public Key Credentials Level 2*. Accessed: Dec. 2, 2021. [Online]. Available: https://www.w3.org/TR/webauthn-2/

[69] FIDO Alliance. (2020). *FIDO UAF Architectural Overview*. Accessed: Nov. 26, 2021. [Online]. Available: https://fidoalliance.org/specs/fido-uaf-v1.2-ps-20201020/fido-uaf-overview-v1.2-ps-20201020.html

[70] FIDO Alliance. (2017). *Universal 2nd Factor (U2F) Overview*. Accessed: Nov. 26, 2021. [Online]. Available: https://fidoalliance.org/specs/fidou2f-v1.2-ps-20170411/fido-u2f-overview-v1.2-ps-20170411.html

[71] N. Vaish. (Jul. 2019). *Why are Enclaves Taking Over the Security World?*. Accessed: Dec. 7, 2020. [Online]. Available: https://fortanix.com/blog/2019/07/why-are-enclaves-taking-over-security-world/

[72] Apple Inc. (2017). *iOS Security*. Accessed: Feb. 15, 2021. [Online]. Available: https://www.apple.com/kr/business-docs/iOS_Security_Guide.pdf

[73] Google. *Android Keystore System*. Accessed: Sep. 21, 2021. [Online]. Available: https://android-doc.github.io/training/articles/keystore.html

[74] European Banking Authority. (Oct. 2019). *Opinion of the European Banking Authority on the Deadline for the Migration to SCA for E-Commerce Card-Basedpayment Transactions*. Accessed: Dec. 13, 2020. [Online]. Available: https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/e8b3ec84-c1c6-4e9a-96ea-3575361dc230/Opinion%20on%20the%20deadline%20for%20the%20migration%20to%20SCA.pdf

[75] E. Union, "Commission delegated regulation (EU) 2018/389," *Off. J. Eur. Union*, vol. 69, pp. 23–43, Nov. 2017.

[76] F. Mennes. (Apr. 2017) *PSD2: Which Strong Authentication and Risk Analysis Solutions Comply With the E's Final Draft RTS?*. Accessed: Nov. 12, 2020. [Online]. Available: https://frederikmennes.wordpress.com/2017/04/19/psd2-which-strong-authentication-and-risk-analysis-solutions-comply-with-the-ebas-final-draft-rts/

[77] V. Haupert and T. Müller, "On app-based matrix code authentication in online banking," in *Proc. 4th Int. Conf. Inf. Syst. Secur. Privacy*, 2018, pp. 149–160.

[78] ENISA. (Mar. 2020). *eIDAS Compliant eID Solutions*. [Online]. Available: https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions/@@download/fullReport

[79] I. Pollari, C. Bekker, and C. Jowell. (2019). *The Future of Digital Banking: Banking in 2030*. KPMG. Accessed: Jul. 1, 2020. [Online]. Available: https://home.kpmg/au/en/home/insights/2019/07/future-of-digital-banking-in-2030.html

[80] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron, and K. Seamons, "A usability study of five Two-Factor authentication methods," in *Proc. 15th Symp. Usable Privacy Secur. (SOUPS)*. Santa Clara, CA, USA: USENIX Association, Aug. 2019, pp. 357–370. [Online]. Available: https://www.usenix.org/conference/soups2019/presentation/reese

[81] M. Kumar and S. Gupta, "Security perception of e-banking users in India: An analytical hierarchy process," *Banks Bank Syst.*, vol. 15, no. 1, pp. 11–20, Feb. 2020, doi: 10.21511%2Fbbs.15%281%29.2020.02.

[82] O. Sarjiyus, N. D. Oye, and B. Y. Baha, "Improved online security framework for e-banking services in Nigeria: A real world perspective," *J. Sci. Res. Rep.*, vol. 6, pp. 1–14, Apr. 2019.

[83] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," *Cryptography*, vol. 2, no. 1, pp. 1–31, 2018. [Online]. Available: https://www.mdpi.com/2410-387X/2/1/1

[84] C. Jacomme and S. Kremer, "An extensive formal analysis of multi-factor authentication protocols," *ACM Trans. Privacy Secur.*, vol. 24, no. 2, pp. 1–34, Jan. 2021, doi: 10.1145/3440712.

[85] I. Velásquez, A. Caro, and A. Rodríguez, "Authentication schemes and methods: A systematic literature review," *Inf. Softw. Technol.*, vol. 94, pp. 30–37, Feb. 2017.

[86] B. B. Gupta, N. A. G. Arachchilage, and K. E. Psannis, "Defending against phishing attacks: Taxonomy of methods, current issues and future directions," *Telecommun. Syst.*, vol. 67, no. 2, pp. 247–267, Feb. 2018.

[87] B. Chaimaa, E. Najib, and H. Rachid, "E-banking overview: Concepts, challenges and solutions," *Wireless Pers. Commun.*, vol. 117, no. 2, pp. 1059–1078, Mar. 2021.

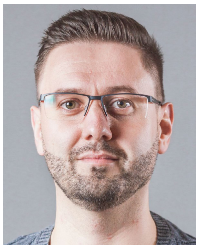
[88] S. Kiljan, K. Simoens, D. D. Cock, M. V. Eekelen, and H. Vranken, "A survey of authentication and communications security in online banking," *ACM Comput. Surveys*, vol. 49, no. 4, pp. 1–35, Dec. 2017.

[89] F. Sinigaglia, R. Carbone, and G. Costa, "Strong authentication for e-banking: A survey on European regulations and implementations," in *Proc. SECRYPT*, 2017, pp. 1–6.

[90] F. Sinigaglia, R. Carbone, G. Costa, and N. Zannone, "A survey on multi-factor authentication for online banking in the wild," *Comput. Secur.*, vol. 95, Aug. 2020, Art. no. 101745.

[91] M. M. Althobaiti and P. Mayhew, "Security and usability of authenticating process of online banking: User experience study," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2014, pp. 1–6.

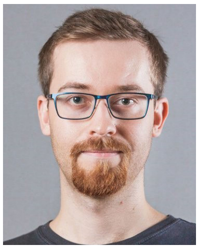
[92] S. G. Lyastani, M. Schilling, M. Neumayr, M. Backes, and S. Bugiel, "Is FIDO2 the kingslayer of user authentication? A comparative usability study of FIDO2 passwordless authentication," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2020, pp. 268–285.



KAMIL MALINKA received the M.S. degree in applied informatics from Masaryk University (MU), in 2005, and the Ph.D. degree in biometrics and anonymity systems from the Faculty of Information Technology, Brno University of Technology, Czech Republic, in 2010. Currently, he is working as an Assistant Professor with the Faculty of Information Technology, Brno University of Technology. He is also working as an IT Architect and a Researcher at MU and a member of the Local Security Research Group Security, Faculty of Information Technology, where he is focusing on computer and network security.

ONDŘEJ HUJŇÁK received the M.S. degree in information technology security from the Brno University of Technology, in 2016, where he is currently pursuing the Ph.D. degree in computer science and engineering. He is a member of the Research Group Security, Faculty of Information Technology, where he is focusing on computer and network security. His research interests include the security of IoT networks and devices, privacy-enhancing technologies, and cyber-physical systems.

PETR HANÁČEK received the M.S. degree in computer engineering and the Ph.D. and Habilitation degrees in computer science from the Brno University of Technology, Czech Republic, in 1988, 1997, and 2003, respectively. He leads the Local Security Research Group Security, Faculty of Information Technology, where he is focusing on computer and network security. From 1987 to 2001, he worked at the Department of Computer Science, Faculty of Electrical Engineering and Computer Science, Brno University of Technology. Since 2002, he works with the Faculty of Information Technology, Brno University of Technology. He is currently the Head with the Department of Intelligent Systems and an Associate Professor with the Faculty of Information Technology, Brno University of Technology.



LUKÁŠ HELLEBRANDT received the M.S. degree in information technology security from the Faculty of Information Technology, Brno University of Technology, in 2016, where he is currently pursuing the Ph.D. degree. He takes part in the security at the Faculty of Information Technology, Information Technology Security Research Group. He works as a Senior Quality Engineer at Red Hat. His research interests include anonymity networks and privacy-enhancing technologies.