25th RSEP International Conference on Economics, Finance & Business
16-17 June 2022, Mercure Paris 19 Philharmonie La Villette Hotel, Paris, France

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-8-6/July 2022

Scheau, M.C., et.al. pp.52-68

Risk-based approach in preventing mobile banking cyber-attacks

Mircea Constantin Șcheau[a], Larisa Găbudeanu[b], Iulia Brici[c], Liliana Apetri[d] & Corina Narcisa Bodescu[e]

[a] *Researcher, European Research Institute, Babeș-Bolyai University, Cluj-Napoca, Romania & Faculty of Automation, Computers and Electronics, University of Craiova, Craiova, Romania*
E-mail: mircea.scheau@ubbcluj.ro , mircea.scheau@edu.ucv.ro
[b] *PhD candidate, Faculty of Law, Babeș-Bolyai University, Cluj-Napoca, Romania*
E-mail: larisa.gabudeanu@ubbcluj.ro
[c] *PhD candidate, Doctoral School of Economics and Business Administration, Babeș-Bolyai University, Cluj-Napoca, Romania*
E-mail: iulia.brici@ubbcluj.ro / Corresponding Author
[d] *European Cybersecurity Organization*
E-mail: liliana.apetri@gmail.com
[e] *PhD candidate, Doctoral School of Economics and Business Administration, Babeș-Bolyai University, Cluj-Napoca, Romania*
E-mail: narcisa.bodescu@econ.ubbcluj.ro

DOI: https://doi.org/10.19275/RSEPCONFERENCES174

Abstract

In the context of a continuous technologization of the world, people create a lot of shortcuts and facilities, but unfortunately they leave room for opportunities to commit cybercrime. The financial and banking industries are two of the sectors affected when it comes to cyber-attacks. Banking products and services are now at our fingertips more than ever. Many of them are compressed in platforms and mobile applications, leading to time saving for customers. Unfortunately, the disadvantage is the risk of compromising their personal information. Over the last decade, a significant number of new vulnerabilities are identified each day. These refer to firmware and software that is provided to customers or used as components to build other software. The purpose of a cyber-attack is generally a financial gain, but it can also include exfiltration of sensitive financial data or identity theft. One of the objectives of our study is to classify several types of cyber-aggressions based on the existing research, with emphasis on identifying the vulnerabilities that facilitate cybercrime. In the financial sector, proper management of vulnerabilities in order to reduce risks is essential. For this reason, the pillar objective was to propose a risk-based approach. Our methodology was based on collecting data and processing statistics on attack techniques and mitigation measures. The analysis identifies criteria for performing the risk assessment in terms of malware actions prevention for mobile banking platforms. The results of the study show that certain types of cyber-attack techniques and vulnerabilities can be addressed by the payment service provider, while others require notifying the customer about the malware presence. In terms of policy implications, the main beneficiaries of the study are banks, financial institutions and their customers as well. Future research on this topic can contribute by making a risk-based approach in terms risk level for each vulnerability.

Keywords: security by design, prevention policy vulnerabilities, risk management, innovation, online banking

Jel Codes: G21, G32, K14, K24, O33

1. Introduction

People are constantly developing ways to make life easier. In the 21st century the changes have been much more pronounced thanks to the intervention of technology. In this age dominated by the principle of the speed of doing things, technology has an essential role in the process of the world's transition from classic to digital. The effects are felt in all existing fields of activity, while others were even arising from digital innovation. There are a lot of factors that underlie digitalization, in addition to the need to facilitate many processes. The latest factor is the COVID-19 pandemic, which has significantly accelerated the technological progress in the last two years. In the literature it is called "the great accelerator" or "the catalyst" (Amankwah-Amoah et al., 2021). Of course, once the effects of digitalization began to appear, whether they were positive or negative, researchers found a new sphere of interest. (More et al., 2016; Jebarajakirthy & Shankar, 2021; Chaudhary et al., 2021; etc).

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-8-6/July 2022

Scheau, M.C., et.al. pp.52-68

In this context, we have channeled our research on certain cyber security aspects in the digitalization in the financial-banking field, with emphasis on the effects it has and, implicitly, on the need to develop a risk management policy of a higher level of efficiency, precisely due to the diversification of the associated risk. In the financial sphere, the digital transformation process supports the increase of the quality of the offered services, the creation of new financing channels, the increase of the level of financial integration, but also the development of a strategic policy in the niche of financial services. In the banking sphere, digitalization has made its presence felt for both front and end-level operations. The facilities are based on various kinds of software that allows transfers, account management, balance consultations, currency conversions, etc. It certainly generates, on the one hand, time saving, both for the client and for the bank employee. On the other hand, the software behind banking applications can sometimes be vulnerable and criminals will certainly take every opportunity in order to unlawfully win a financial gain or to steal data and identities.

One area of interest from a technological perspective, but also from a regulatory and cyber security perspective is the use of remote mechanisms for payments. This has been the focus in the European Union in the past decade, with the most recent legislation in this respect (the Payment Services Directive 2, Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market ("PSD2")). Among the cyber security obligations under PSD2, article 95 establishes the obligation for payment service providers to set up an internal framework concerning appropriate mitigation control to manage the operational and security risks related to the payment services they provide.

Further, there are specific requirements concerning transaction monitoring (Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication) in terms of identifying fraud scenarios and malware presence on the client's device.

These two legal requirements are setting the tone for the obligation of organizations (such as banks or other payment service providers) to analyze in a risk-based approach the possibility of a payment being made by cyber-criminals (manually or automatically using the malware installed on the device of the client).

The practical implications of these legal requirements stem from technical and economic aspects. On the one hand, gathering the relevant intelligence and using third party solutions to properly identify the presence of malware on the client's device. On the other hand, taking into account the risk appetite, the costs and the prioritization of mitigating controls, an organization has to properly address the identified risks.

Existing literature details either technically, the known malware types and their implications or controls to prevent them or details other security obligations under PSD2, such as the automatic fraud scenario identification based on the payment behavior of the client or the strong customer authentication practical implementation.

Therefore, this research paper aims to fill the gap in terms of literature on the cyber security mechanisms to be taken by payment service providers for malware prevention and detection in the context of payments made by client remotely on their devices, while establishing a framework for addressing the related risk through prioritization of controls to be implemented.

The research paper includes the analysis of the banking malware indexed by MITRE, especially in terms of location where this has been used, interval it was used (or re-used), cyber-attack tactics and techniques. From this analysis, specific criteria that can be taken into account by payment service providers has been extracted, with the aim of creating a framework that can be updated continuously based on new banking malware that appears or which spreads its use to other countries/continents.

The results of this research paper represent the criteria for risk prioritization together with the relevant mitigating controls and the framework that can be used also in the future by the payment service providers.

The original approach in this research paper represents the combining of existing details on malware tactics and techniques and relevant mitigating controls to establish a framework useful to payment service providers for their risk-based approach of the legal requirements concerning identification of malware when payments are being performed by their clients. Thus, this framework can be used to prioritize changes to payment applications and to allocate budgets efficiently in order to address high-risk vulnerabilities with priority and to ensure the safety of the payments made by clients.

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-8-6/July 2022

Scheau, M.C., et.al. pp.52-68

In the following, the information will be presented in the form of sections that divide our research into areas of interest: existing literature, types of attacks, identified vulnerabilities, proposed approach for risk assessment and risk response and conclusions. Section 2 is a review of the literature, in which we have synthesized, in a critical manner, the most relevant studies related to the chosen topic. These studies refer both to the classification of cyber-aggressions and to the associated risks identified by other authors. The purpose of this section is to identify the level to which the research on the chosen topic has reached until now and to find the gap that we will address in our study. Section 3 presents the most recent and the most common types of cyber-attacks on banking applications (both belonging to banks and fintech). In this section can be also found the examination of the vulnerabilities and the proposal of the risk management policy in order to combat them effectively. Section 4 presents the risk mitigation mechanisms and controls that can be taken into account by organizations based on their existing IT landscape as well. Section 5 presents the results of the study, with evolutionary approaches, but also econometric estimation. The last section gathers our study by concluding the results we have reached, but also by proposing potential solutions to the identified issues. At the same time, at the end of the study, have been integrated the limits of the study and the future line of research.

2. Literature Review

The field of online banking is increasingly discussed in the recent years' literature. If at first it included topics such as the methods that make life easier for customers and employees in the financial-banking field, such as online banking platforms, but also applications developed by banks (Shankar & Rishi, 2020), recent literature explores the problematic of their information security vulnerabilities (Adam et al., 2021).

In this section we aim to provide an overview of the literature that refers to the topic that we will address in this paper. We start our research by presenting our processing done using VOSviewer which is a software tool used for constructing, but also for visualizing bibliometric networks.

The cyber-attack and also security standards concerning internet banking have increased their visibility only in the last decade, consequently a few studies on security in relation to mobile banking have been conducted and published in journals with a significant impact factor. Our assertion is supported by the number of articles, studies and books identified in the Web of Science following the searches for the associations of terms 'online banking' and 'security' or 'risk'.

Thus, from the papers published on Web of Science (until April 2022, the period of our research development) on 'internet banking' in correlation with 'security' or 'risk', by the search field: title, author, keywords and abstract, we

have identified 907 papers addressing the issue of internet banking in connection with security and 730 works on. The processing with the VosViewer software of the 907 articles, previously mentioned, resulted in 69 keywords used (at least 10 occurrences) are illustrated in Figure 1 below.

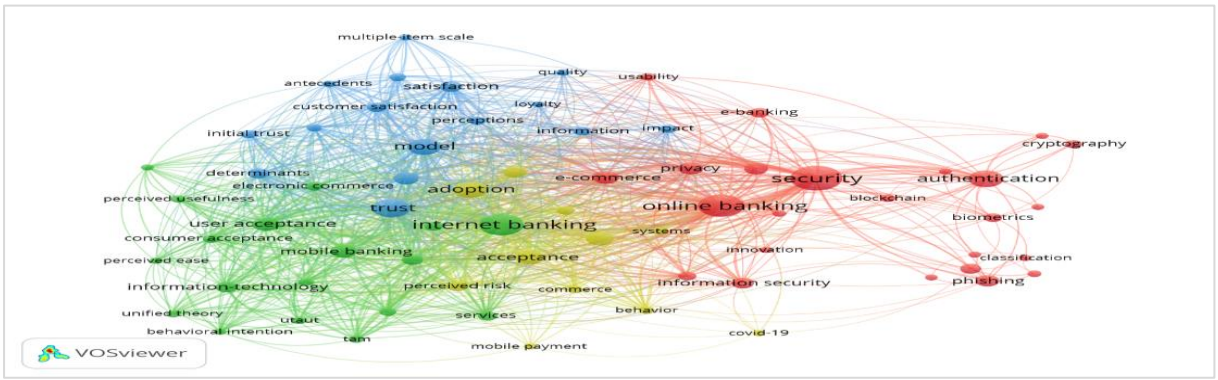

Figure 1. Map of key word used in articles on online banking and security

Source: Authors' processing

Most of the identified terms refer to the transition from classical banking to digital banking (e.g. 'internet banking', 'online banking', 'mobile banking'), including all areas in which this event has produced changes (e.g. 'e-commerce', 'e-banking', 'mobile payment'). Also, among the identified terms are mentioned the intermediate factors that

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-8-6/July 2022

produced fluctuations in the level of digitalization in the financial-banking field (e.g. 'Covid-19'), but also the less good perspective of this change, respectively the occurrence of crimes (e.g. 'phishing').

From the point of view of the distribution of the keywords used over time, the map below shows that in the recent years (marked in yellow color) the most commonly used are the following terms: 'blockchain', 'perceived risk', 'behavioral intention' (Figure 2).

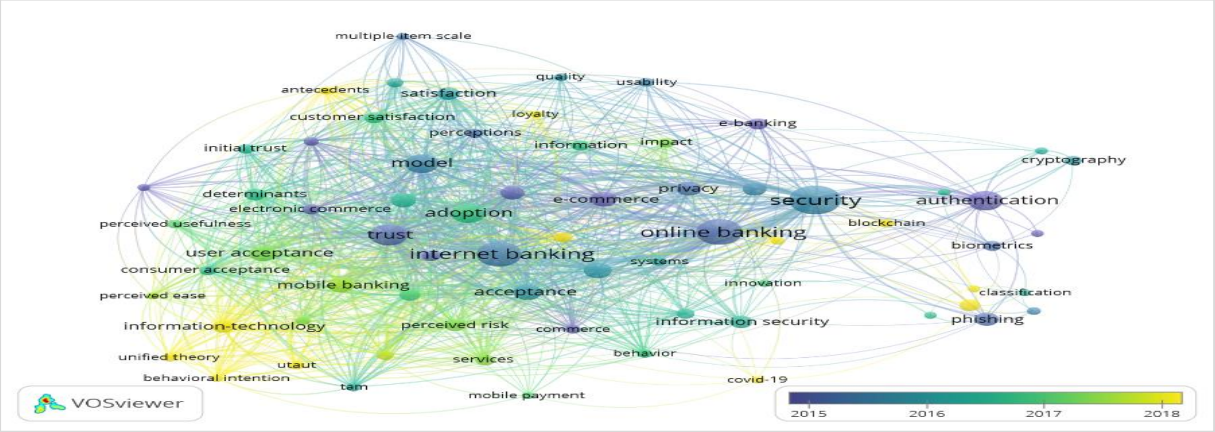

Figure 2. Map of time distribution of key word used in articles on online banking and security

Source: Authors' processing

We can deduct from the results of the processing in Figure 2 that the most frequently used terms in recent years refer to the most recent concerns in the financial-banking sector. On the one hand, the rapid development of cryptocurrency transactions and, at the same time, the use of blockchain technology can lead to data leaks and increases in the level of financial risk. Those who commit such criminal acts are monitored and analyzed, so that we can talk about identifying a specific behavior.

Further, abstract frequently used terms (150 terms selected by criteria with at least 20 occurrences) were grouped in 2 clusters (Figure 3) according to the number of occurrences and relevance of the words connected in these articles.

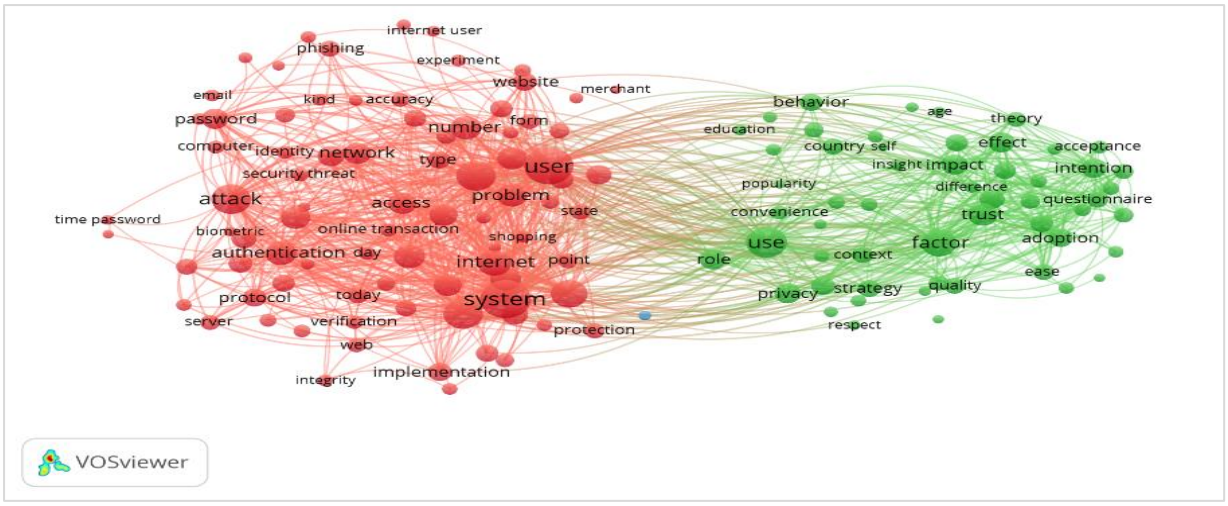

Figure 3. Map of term used in articles on online banking and security

Source: Authors' processing

As we would have expected before making this analysis, this time the terms are much deeper in the addressed issue. In the abstracts of the studies, the information resulting from the existing research is synthesized, therefore the terms refer to the technical part of the use of technology in the financial-banking field (e.g. 'biometric', 'server', 'security threat'), but also to the approach subject analysis (e.g. 'theory', 'factor', 'strategy').

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-8-6/July 2022

Scheau, M.C., et.al. pp.52-68

In what concerns the area of origin of the existing studies, in figure 4 below we find the top 10 countries/regions with the most publications that refer to the subject of our research.

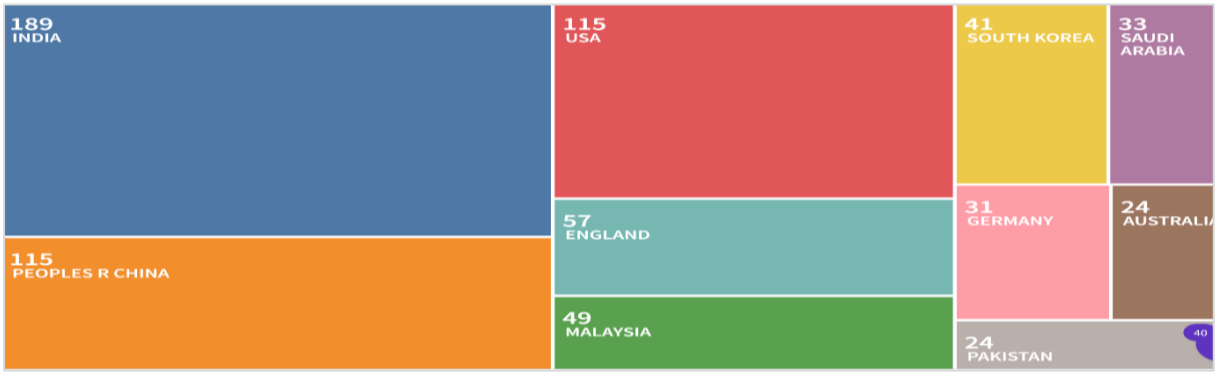

Figure 4. Top 10 countries/regions of articles (Web of Science analyze)

Source: Authors' processing

A higher number of studies in a certain area can be determined by a high level of the population, implicitly by the high number of active researchers. But we can look at things from another perspective, leading us to the assumption that in these countries or regions can take place the highest number of financial crimes, being the places with the most possible opportunities to make research on the subject. In the following, we will make an assessment of the most relevant existing resources, trying to capture the stage of the literature and the conclusions reached by the other authors.

In the study of Scheau et.al (2020), the authors show that in 2019 the number and intensity of reported attacks, mainly ransomware, increased compared with previous year, in many areas including financial field. Also, the rapid emergence and evolution of high-speed information networks could lead to a cyberwar and it needs concerted efforts to reduce the imbalance generated by the benefits of illegal growth, supported by innovation.

Credit card fraud causes significant financial losses to merchants and banks (Achim and Borlea, 2020). According to Robertson (2016), the worldwide card fraud losses rose from $7.6 billion in 2010 to $21.81 billion in 2015, or 300% over 5 years. By 2020, global card fraud losses are expected to reach $31.67 billion. The proceeds of this fraud are known to finance terrorism, arms and drug crime (Ryman-Tubb et al. 2018).

Regarding the issue of the link between online banking and cyber-attacks, the literature has been augmented with the help of a relevant study (More et al., 2016) which describes both the advantages and disadvantages of the evolution of technology in the field of e-banking. The aim of this study was to review the stage of adaptation of the banking field to online platforms, but with a focus on cyber-attacks caused by vulnerabilities in the online space. The findings of the study showed that cybercrime is on an upward trend, and criminals are usually male, between the ages of 18 and 30. The study's proposals are aimed at developing a risk management policy in the online space. Studying on the same line of research, closer to our days we can identify in the literature a study referring to the impact of different demographic factors on the preference of using online banking facilities in everyday life (Chaudhary, 2021). The research was done in the form of a questionnaire. The study shows that most of the online banking users are male, graduate of university / post university studies.

A similar study of Achim et al. (2021) show a wide literature review on the advantages and disadvantages of technologies on financial crime. In addition, this study investigate the impact of technology on the level of the economic and financial crime, using data for 185 countries for the period 2012–2015. The authors find clear evidence that increased technology reduces the size of the economic and financial crime, thus the advantages of technologies are more higher than disadvantages . In addition, the study of Achim et al (2021) find that Research and development expenditure (% of GDP) matter more in reducing the financial crime in low income countries compared to high income countries.

A relevant study (Shankar & Rishi, 2020) explored the extent to which the convenience provided by the online domain has an impact on the use of mobile banking services. Following a study based on a questionnaire, it shows that due to convenience, the user tends to use mobile banking services and these intentions materialize in most cases. These findings help banks to optimize their mobile banking platforms to attract as many users as possible,

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-8-6/July 2022

but also to retain existing ones. The following year, one of the authors continued his study with another researcher (Jebarajakirthy & Shankar, 2021). This time the methodology is based on the elaboration of structural equations. The results of the study indicate an obvious impact of online comfort and convenience on the intention to adopt mobile banking.

Talking about convenience and sustaining that the COVID-19 pandemic was a key factor in increasing the level of digitalization, we identified another study (Amankwah-Amoah et al., 2021) in which the authors call the pandemic "the great accelerator" of lifestyle, working manner, business strategies. The study shows that the adoption of technology may encounter obstacles of external interests (nostalgia, combining private and professional life), but it can also represent a benefit (time saving, convenience of working from home). The study concludes that adopting technology in the depths of a business can present risks that might be difficult to control. Another relevant study (Windasari et al., 2022) claims that during the pandemic, cashless payments were encouraged, so there is a complete digitization of banking services between generations Y and Z. The study analyzes the relationship of eight variables in context: use of e-banking (economic value, social influence, ease of use, firm reputation, characteristics, promotion, curiosity, reward). The results show that creating an attractive and easy-to-use digital banking interface would make it easier for customers to use it. However, an additional contribution is needed, namely: rewards, uniqueness of characteristics and credibility.

In a study on mobile banking applications (Hayikader et al., 2016), the authors examine the causes of financial losses due to vulnerabilities in the security structure of banking applications. The authors explore each issue identified and come up with proposals to improve security policy. These include: traditional access control to protect against compromises using active passwords on screen lock in idle time, the source of the application using a custom signature of the author to differentiate their identity, encryption to avoid using data from lost / stolen devices , isolation to restrict an application's access to data on a device, permission-based access control to restrict each application from accessing data without permission.

Another interesting study considers the risks associated with mobile applications (Abdullah et al., 2022). The authors study the calculation of the risk of Android applications, but the conclusions can be generally valid for the security of any application. They evaluate predictive security risk analysis based on machine learning. The authors look for the sources of vulnerabilities, finding that there are some useful and effective prediction models, but more detailed research is needed to fix those security issues.

In terms of classifying the types of malware that digital banking faces, another important study (Black and Opacki, 2016) presents the latest, but also the most dangerous families of malware (Zeus, Citadel, Vawtrak, Dridex, Rovnix, Neverquest). To combat these types of malware it is necessary to understand how they work in order to create a reverse technology. The study is based on the proposal of anti-analysis techniques to eliminate all these variants of malware. Several studies have been developed on the detection of various types of malware and how they work (Sachdeva et al., 2018; Kadir et al., 2018; Mira, 2020; Kumar et al., 2020). Each of them has a distinct vision of the problem, but their purpose is common. Sachdeva et al. propose to differentiate Android applications by classes in order to extract the most important security features. Based on penetration tests, a confidence level of 81.8% was found, which means that there is still a margin of risk. Kadir et al. propose a taxonomy on the types of malware that exist, trying to understand their mode of action in order to find an effective way to combat them. In their study, they identified 32 families of malware. They propose a model that allows the automatic classification of malware based on the correlation of the different symptoms they produce on the attacked devices. Mira focuses its study on classifying existing types of malware, but also on ways to attack them. Kumar et al. come to support this concept and analyze malware detection techniques on mobile devices. The study is a review of changes in attack techniques over time. The paper examines existing viruses and proposes detection solutions for each of them, but also discusses the extent of the results of a cyber attack produced by the investigated malware types.

In what concerns the risks caused by the gaps in the security of Android applications, a study (Yoo et al., 2019) comes to complete the literature, by highlighting the importance of the existence of an active risk management policy. The study presents a visual analysis system using the permissions of the application. It stores personal security information and uses it to analyze an associated risk life diary. The system proposed by the authors allows observation, understanding, but also risk mitigation.

Regarding the issue of risk management in the financial and banking field, we have identified a study that provides a model of risk management policy for directors, managers, boards of banks (Adam, 2021). Unfortunately, this

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-8-6/July 2022

model to follow refers to the risks encountered in classical banking, not in digital one. Such a model would be necessary in order to be able to quantify the existing risks and to be able to eradicate them.

Also regarding the existing risks, another captivating study (Haidar and Almustafa, 2022) highlights the analysis of cyber-attacks on e-banking platforms based on semantic techniques. They collect and integrate information using an ontology that helps to understand risks more quickly. The study focuses on the analysis of such ontologies that have already been tested, finally proposing one to classify the attacks on electronic banking services according to similarities in their way of action.

The literature referring to the chosen field is very comprehensive, covering the side of the use of online banking platforms and applications, but also of the possible existing risks. As we already have exemplified above, there are many studies that capture the existing types of cyber-attacks on online banking facilities, but what we have noticed is that very few researchers have approached the direction of developing a risk management policy. For this reason we aim to cover this part of literature that has been less exploited. In the following we will present a more current typology of cyber-attack forms on virtual banking services and we will capture the vulnerabilities associated with e-banking platforms and apps used by hackers in order to create a compromise or theft. At the end of the next section we want to propose solutions to improve the effects of the crimes that already took place, but also to come up with ideas to combat or stop future events of this type.

3. Data and methodology

This research paper analyzed the data on banking malware cyber-attacks and on cyber-attack techniques used by banking malware. Further, the analysis identifies the criteria to be used for mitigating the identified risks in a risk-based approach. There are certain software solutions that work as an add-on to the mobile banking application to detect presence of malware of the user's mobile device or any other risk factors (e.g., rooted device). These are generally updated with the latest malware signatures to properly identify threats. However, this is only one prevention method located at a specific level of the mobile banking application's architecture and it only addresses well known attack vectors from known malware families. Further, complex security solutions scanning for a significant number of malware families throughout the use of the mobile banking application may lead to latency in performance of services. Thus, a defense in depth approach is needed to mitigate risks related to banking malware on mobile devices.

This research paper is aimed at identifying main criteria to have in mind when performing the risk assessment in terms of malware prevention for the mobile banking application. To this end, we have analyzed multiple statistics related to attacks on mobile banking applications (names of malware, attack techniques and related mitigation measures) together with statistics concerning coverage of certain malware types. Then we deep dived into the main criteria resulting from this statistical analysis to further understand the most relevant criteria for risk assessments in terms of prioritization of risk addressing together with the main prevention mechanisms to be set in place with priority. Given the wide range of different banking malware, one approach that can be taken is a risk-based approach in which identified vulnerabilities of the internet banking application or of the user's device when using internet banking are analyzed and mitigated based on certain criteria, respectively, the impact (negative consequences on the customers and on the payment service provider) and the probability of such impact occurring. Of course, in most cases, the impact and probability can be estimated by expert knowledge of security experts, as complex statistical data addressing this is not available as it can differ significantly based on internet banking solution used, other payment service provider controls in place and on the user's device.

The main characteristic of a risk-based approach is to identify the relevant potential negative consequences concerning the use of and payment through internet banking applications (web or mobile) together with the characteristic of the event that can trigger such consequences. This is named a risk scenario. Such information about banking malware and their techniques can be obtained from multiple sources. First, there are publicly available information in this respect published by security researcher. This is the option we used for this research paper in which we referenced data published by Mitre. Secondly, specific vendors of threat intelligence provide detailed information on recent banking malware, including vendors that offer solutions which can be used directly by payment service providers embedded in their internet banking applications in order to obtain relevant data directly from their customers. Thirdly, there are community sources, which include public authorities and threat intelligence communities in the financial sectors that share relevant information. Further, depending on details concerning existing controls that mitigate certain types of cyber-attacks, the impact and probability can be adjusted to reflect this. Subsequently, based on the risk level resulting from the risk assessment and the risk appetite of the

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-8-6/July 2022

payment service provider, the mitigation mechanism and approach is established. For the purpose of this research paper, we have included certain mitigation measures as well. This is a circular process that can be performed internally by the payment service provider, which can be performed periodically, either at regular intervals or also when a new types of relevant banking malware appears.

4. Results and discussions

4.1 Data concerning banking malware attacks

According to a database developed by Eurostat (Eurostat, 2020) for the European Union member states, in the period 2015-2020, an indicator called 'Internet use: Internet banking' was calculated using the questionnaire method (Figure 5 below). This index expresses the percentage of the individuals which use internet banking services, more precisely within the last 3 months before the survey was launched. In this situation, internet banking represents electronic transactions with a bank for payment or searching for account information. Throughout the analysis period, the countries with the highest levels of adaptability in terms of internet banking use are the Nordic countries (Denmark, Finland) and the Netherlands. On the other hand, the last places in the charts are occupied by countries such as Greece, Romania and, on the last place in the ranking, Bulgaria. The conclusion of this study could lead us to think that the indicator may largely depend on the degree of development of the country for which it is calculated. The level of usage of internet banking in a specific country is relevant in terms of internet banking cyber-attack risks. For instance, if a high percentage of the population is using internet banking, theoretically user are going to be more targeted by banking malware. Further, if the users have only in recent years started to use internet banking, it may entail that the users and the payment service provider do not have sufficient experience in handling banking malware, and, thus, may be easier targets for the cyber-criminals. Figure 5. Internet use: Internet banking 2015-2020, EU member states

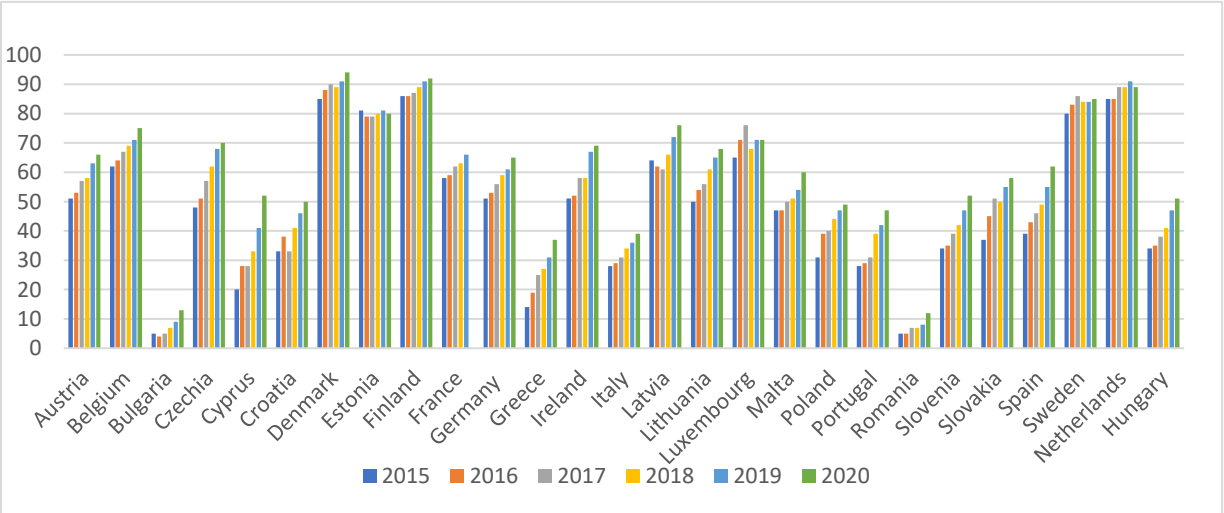

Figure 5. Internet use: Internet banking 2015-2020, EU member states

Source: Author's processing based on Eurostat dataset

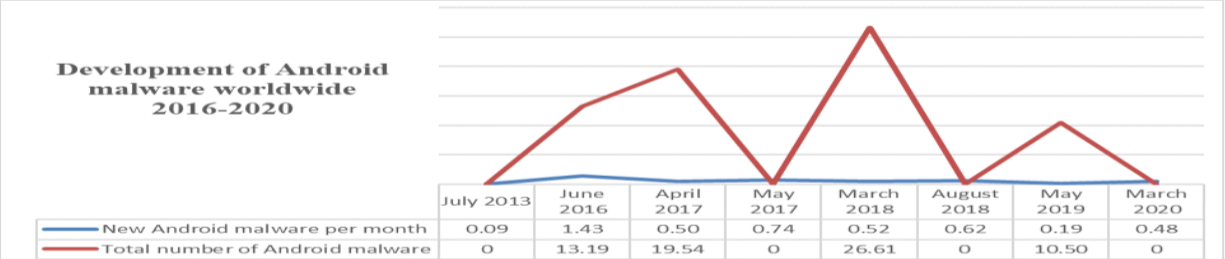

Figure 6. Development of Android malware worldwide 2016-2020

Source: Author's processing based on Statista data

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-8-6/July 2022

Another study published by Statista and powered by AV-Test, refers to a Security Report data which allows us to see how various types of Android malware developed worldwide, in the period 2016-2020 (Statista, 2020[1]). In Figure 6 above we can see marked in red the total number of types of Android malware that were developed from the reference point, July 2013, to March 2020.

The maximum point of expansion was reached in 2018 after which the level decreased, which may mean that effective methods of combating these types of malware have been discovered from that point. Marked in blue are the new types of malware that have appeared from month to month. This time, the maximum level was reached in 2016, and the values from the next period do not show alarming increases. This type of analysis is useful in order to understand the relevant of the operating system on the numbers of banking malware cyber-attacks and also in order to monitor spikes in banking malware campaigns. It is interesting to see that each year there is a certain month with peak malware values. Generally, this is in spring (e.g., April 2017, March 2018, May 2019). It may be that in this period of the year there are a lot more mobile applications being installed or used or a lot more online content being shared between users. Such situations are optimal for malware propagation due to the fact that a message sent by a cyber-criminal or a mobile application developed by a cyber-criminal can go undetected due to the large amount of messages and actions of the users. Searching deeper on these fluctuations, it seems that the highest rates are due to the appearance of a new malware code programmed for all types of Android devices called 'Hiddad'. It was a type of trojan in 2018, reaching the top of the most dangerous types of malware. It works by hiding from Google Play apps and becomes undetectable by operating system security apps. On the affected devices, Hiddad displays full-screen ads allowing the perpetrators to extort cash in this manner.

Another relevant publication from Statista refers to a study developed by Kaspersky (Statista, 2020[2]). It informs the general public about the countries most targeted by banking malware attacks in 2020. This top 10 is led by Uzbekistan and Turkmenistan, with rates between 8.6 and 10.4% incidence of attacks on internet banking platforms (Figure 7). At the opposite end are Guatemala and South Korea.

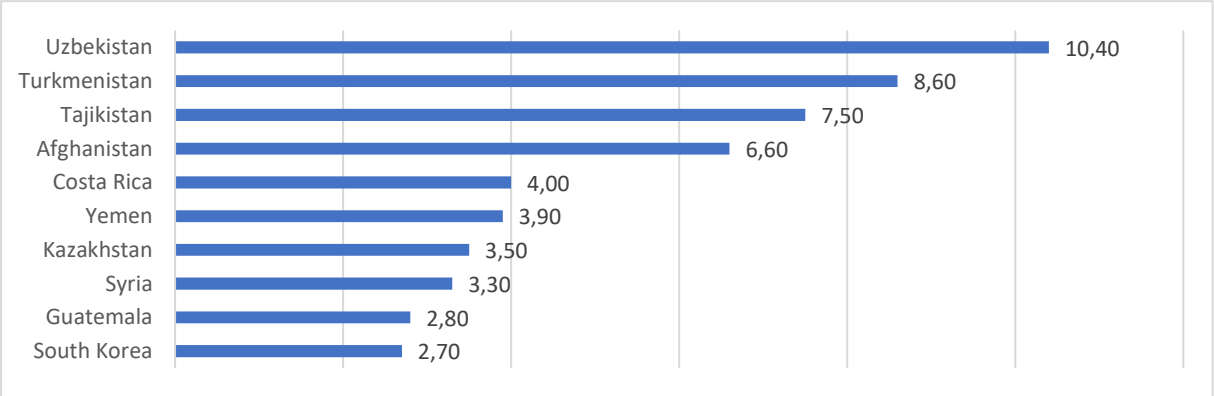

Figure 7. Banking malware attack rate 2020, by country

Source: Author's processing based on Statista data

The high levels are explained by a gap in cybersecurity policies, which was also evidenced by a recent publication by Dentons, a global law firm, which says that the first cybersecurity law in Uzbekistan was proposed only on April 15, 2022, following to become active on July 17, 2022. This type of information is relevant in order to understand the geographical relevance in banking malware cyber-attacks. In terms of typology, regarding the most common types of banking trojans reported in 2020, another Statista publication (Statista, 2021) shows that the greatest proportion of malware attacks from the financial sector was represented by family Dridex (26%) followed by Trickbot (23%). The other common types are illustrated in the Figure 8 below.

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-8-6/July 2022

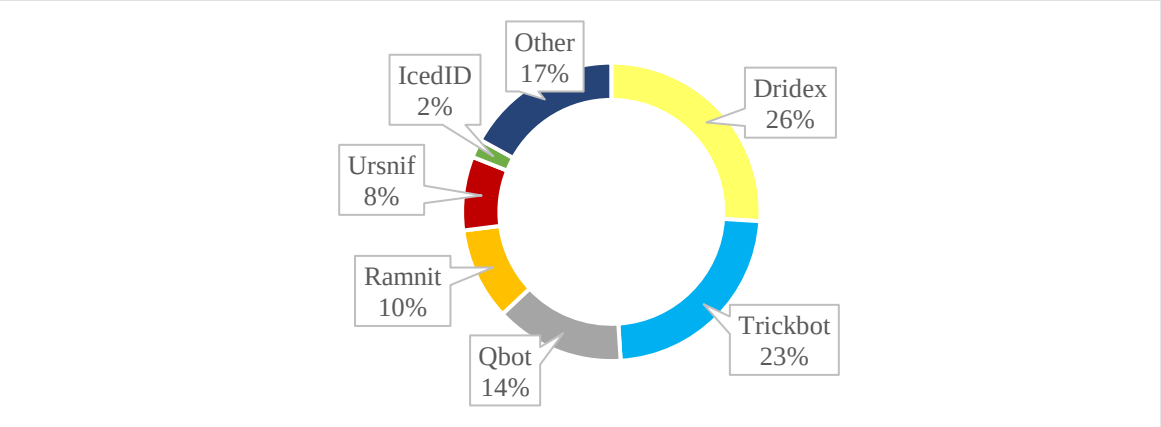

Figure 8. Most prevalent banking trojans worldwide in 2020, by type

Source: Author's processing based on Statista data

The data come from a Cyber Security Report developed by Check Point Software Technologies and they represent the aggregated answers of a survey held between January and December 2020. Such information is useful in order to focus on the most wide-spread banking malware, as the probability of this infecting user devices is higher than other types of banking malware.

This report provides a wide analysis of the current trends in the cyber domain. According to the last worldwide problems, the report contributes with recommendations on how to prevent the challenges of the digital rise during the pandemic. The analysis is based on statistics and detailed explanations of global vulnerabilities. Also, according to this report, there exist 100000 malicious websites and 10000 malicious files per day around the world. Also, at worldwide level, a percentage of 87% of organziations have faced one of this threats because of an existing vulnerability. From these organziations, a percent of 46% have at least one employee who accidentally downloaded a malicious mobile app.

The below information provides an overview of the main techniques used by banking malware in various stages of the cyber-kill chain during a cyber-attack. We have highlighted the techniques that are used by multiple banking malware. It is interesting to see that there are certain key techniques that are generally used by banking malware. This can entail that there are certain vulnerabilities usually present in most internet banking applications (and related back-end thereof). Of course, depending on the banking malware and on the device characteristics of the customer, certain controls can be implemented and certain cannot.

It is also interesting to see that existing or former banking malware is re-used by novel types of banking malware. In addition, certain mutations take place when existing banking malware is used as malware as a service by cyber-criminals that do not have technical experience or for efficiency purposes. In certain cases this malware as a service is bundled with other types of malware or is enhanced by using other types of malware.

Such use of certain techniques in multiple banking malware is useful also for the payment service provider, as the payment service provider can focus on mitigating the widely used techniques with priority.

4.2 Analysis of banking malware techniques

The below data analysis includes data from Mitre concerning malware software, out of which only the malware marked as banking malware was included in the analysis.

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-8-6/July 2022

Scheau, M.C., et.al. pp.52-68

Table 1. Top techniques used by more than 5 banking malware

Technique/Malware	Anubis	Asacub	Cerberus	Defensor ID	Dridex	Dyre	Emotet	EventBot	Exobot	Ginp	Grandoreiro	Gustuff	IcedID	Javali	Melcoz	Metamorfo	QakBot	Red Alert 2.0	Riltok	Rotexy	TrickBot	TrickMo	Ursnif	Zeus Panda	Grand Total
Application Layer Protocol: Web Protocols		1	1	1	1	1		1	1		1	1	1			1	1	1	1	1	1	1	1	1	19
System Information Discovery	1	1	1		1	1		1	1		1	1	1			1	1		1	1	1	1	1	1	18
Obfuscated Files or Information		1	1		1		1	1		1	1	1	1			1	1	1		1	1	1	1	1	17
Software Discovery	1		1	1	1	1		1		1						1	1	1	1	1		1			13
System Network Configuration Discovery		1				1		1	1		1	1					1		1	1	1	1			11
Ingress Tool Transfer						1					1		1	1	1	1	1				1		1	1	10
Input Capture: GUI Input Capture	1		1					1	1	1		1				1		1	1	1					10
Process Discovery	1						1				1			1		1	1			1	1		1	1	10
Protected User Data: SMS Messages		1	1					1	1	1		1						1	1	1		1			10
Input Capture: Keylogging	1		1					1	1		1	1				1	1							1	9
Protected User Data: Contact List	1	1	1						1	1		1						1	1	1					9
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder							1				1		1			1	1				1		1	1	8
Native API		1			1						1		1			1	1				1		1		8
Screen Capture	1			1				1		1						1						1	1	1	8
SMS Control	1	1	1						1	1								1		1		1			8
User Execution: Malicious File					1		1				1		1	1		1	1				1				8
Virtualization/Sandbox Evasion: System Checks	1		1			1				1	1						1			1		1			8
Browser Session Hijacking					1						1		1		1		1				1		1		7
Command and Scripting Interpreter: Visual Basic							1				1		1	1		1	1						1		7
Data from Local System	1									1		1					1				1	1	1		7
Deobfuscate/Decode Files or Information						1					1					1	1				1		1	1	7
Exfiltration Over C2 Channel						1	1				1					1	1				1		1		7
Credentials from Password Stores: Credentials from Web Browsers							1				1			1	1		1				1				6
Encrypted Channel: Symmetric Cryptography					1			1								1	1			1	1				6
Impair Defenses: Disable or Modify Tools	1		1								1					1	1				1				6
Input Injection			1	1						1		1							1			1			6
Modify Registry											1					1	1				1		1	1	6
Phishing: Spearphishing Attachment							1						1	1		1	1				1				6
Phishing: Spearphishing Link							1				1			1	1		1				1				6
Software Packing							1					1	1			1	1				1				6
System Binary Proxy Execution: Msiexec											1		1	1	1	1	1								6
GRAND TOTAL	11	8	12	4	8	8	10	10	8	10	20	11	12	8	5	21	25	7	8	12	20	11	14	10	273

Source: Author's processing based on Mitre.org data

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-8-6/July 2022

Scheau, M.C., et.al. pp.52-68

Table 2. Top techniques used by more or equal then 10 banking malware

Technique/Malware	Anubis	Asacub	Cerberus	Defensor ID	Dridex	Dyre	Emotet	EventBot	Exobot	Ginp	Grandoreiro	Gustuff	IcedID	Javali	Melcoz	Metamorfo	QakBot	Red Alert 2.0	Riltok	Rotexy	TrickBot	TrickMo	Ursnif	Zeus Panda	Grand Total
Application Layer Protocol: Web Protocols		1	1	1	1	1		1	1		1	1	1			1	1	1	1	1	1	1	1	1	19
System Information Discovery	1	1	1		1	1		1	1		1	1	1			1	1		1	1	1	1	1	1	18
Obfuscated Files or Information		1	1		1		1	1		1	1	1	1			1	1	1		1	1	1	1	1	17
Software Discovery	1		1	1	1	1		1		1						1	1	1	1	1		1			13
System Network Configuration Discovery		1				1		1	1		1	1					1		1	1	1	1			11
Ingress Tool Transfer						1					1		1	1	1	1	1				1		1	1	10
Input Capture: GUI Input Capture	1		1					1	1	1		1				1		1	1	1					10
Process Discovery	1						1				1			1		1	1			1	1		1	1	10
Protected User Data: SMS Messages		1	1					1	1	1		1						1	1	1		1			10
GRAND TOTAL	4	5	6	2	4	5	2	7	5	4	6	6	4	2	1	7	7	5	6	8	6	6	5	5	118

Source: Author's processing based on Mitre.org data

4.3 Risk-based approach in malware detection and prevention on user devices

According to the Guidance for a risk-based approach for the banking sector (The Financial Action Task Force, 2014), a risk-based approach in preventing mobile banking cyber-attacks means that main players than competent authorities and financial institutions (banks, FinTech's, payment services providers) should identify, assess , but also understand the cyber-attacks risks to which they are exposed and develop preventing measures to those risks in order to mitigate them effectively. An effective RBA should be based on efficient procedures which provide appropriate information on the results of the risk assessments to all relevant competent authorities, financial institutions and other interested parties.

According to the legal obligations, the organizations falling under the PSD2 should ensure that they detect any malware on the device of the client.

This is rather difficult, as the malware infecting is dependent on user devices, which cannot be controlled by the organization and to which the organization has limited information about and limited access.

First risk-based approach category about banking malware to be had in mind by an organization is the country or continent in which the banking malware is used. Generally, a banking malware is used in one geographical area. However, there are some malware types used all over the world. In addition, there are some cases in which malware from one geographic area is used in other areas, especially in case of malware as a service. In this case, the cyber-criminals that use the malware as a service do not have to have significant technical knowledge to use the malware.

Further, period of activity is also important. Generally, one version or one type of malware is active for a limited amount of time. However, there are also cases in which the malware is re-used after a period of time has passed since it ceased to be used. Such information is generally publicly available after the malware has been identified by security researchers.

The number of infected devices for a specific banking malware is also very relevant in order to understand on the one hand if the infection is at the beginning (and has not reached its peak) and, on the other hand, if the infection is just limited and it will not be spreading.

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-8-6/July 2022

The operating system targeted by the banking malware is also important in order to understand the probability of a banking malware to target a specific internet banking application. For instance, there are specifics for mobile applications.

In addition to the above, there are specific criteria that can be obtained by the payment service provider from analyzing the device of its clients, for instance, settings that are usually changed by malware, applications installed on the device that could be infected with malware or files whose hashes correspond to malware hashes.

Further, for the impact of the identified risk, there are different manners in which a technique can be used during a cyber-attack and difficulty in mitigating against it.

Mitigations controls related to malware should be taken by mobile providers as wells as by the clients.

A mobile application provider should consider adding when developing an application for mobile banking the following controls:

- Identify and protect sensitive data on the mobile device. If data are stored on the device, encryption technology provided by a trusted source should be used.
- Ensure that sensitive data are protected while in transit. Mobile banking applications should enforce the use of an end-to-end secure channel such as secure sockets layer/transport layer security (SSL/TLS) and use strong encryption.
- Implement user authentication, authorization, and session management correctly. Require appropriate-strength user authentication, for example, multifactor versus strong authentication. Physical tokens or voice, fingerprint, or behavioral authentication factors may be appropriate. Banks should have transaction monitoring in place that would allow detecting unauthorized or unusual or fraudulent payment transaction. This monitoring mechanism should take into considerations at least the following: a list of compromised or stolen authentication mechanism, the amount of the transaction, fraud scenarios known, signs of malware infections in the session of authentication, a log of the use of access device.
- Secure data integration with third-party services and applications. Ensure that mobile banking applications and code are tested, come from a reliable source, have supported maintenance, and have no back-end malware (for example, Trojans).

In the table below are presented the security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed related to mobile attacks for banks and clients.

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-8-6/July 2022

Table 3. General mitigating controls related to mobile

Name	Description
Application Developer Guidance	This mitigation describes any guidance or training given to developers of applications to avoid introducing security weaknesses that can have an adversary effect
Attestation	Enable remote attestation capabilities when available and prohibit devices that fail the attestation from accessing enterprise resources.
Deploy Compromised Device Detection Method	A variety of methods can be used to enable enterprises to identify compromised devices, whether using security mechanisms built directly into the device, third-party mobile security applications, enterprise mobility management (EMM)/mobile device management (MDM) capabilities, or other methods.
Encrypt Network Traffic	Application developers should encrypt all of their application network traffic using the Transport Layer Security (TLS) protocol to ensure protection of sensitive data and deter network-based attacks.
Enterprise Policy	A mobile device management (MDM), system can be used to provision policies to mobile devices to control aspects of their allowed behavior. It should exist processes requiring identifications & remediations of vulnerabilities in servers and applications.
Interconnection Filtering	In order to mitigate Signaling System 7 (SS7) exploitation, the Communications, Security, Reliability, and Interoperability Council (CSRIC) describes filtering interconnections between network operators to block inappropriate requests.
Lock Bootloader	On devices that provide the capability to unlock the bootloader perform periodic checks to ensure that the bootloader is locked.
Security Updates	Install security updates in response to discovered vulnerabilities. Deploy anti Denial of Service measures for critical servers hosted in data servers & cloud.
System Partition Integrity	Ensure that Android devices being used include and enable the Verified Boot capability, which cryptographically ensures the integrity of the system partition.
Use Recent OS Version	New mobile operating system versions bring patches against discovered vulnerabilities and security architecture improvements that provide resilience against potential vulnerabilities or weaknesses that have not yet been discovered.
User Guidance (Client guidance)	Describes any guidance or training given to users to set particular configuration settings or avoid specific potentially risky behaviors. Banks should post on their website techniques to prevent clients from getting manipulated into disclosing confidential information. Client should use only official contact information. Clients should use strong PIN, PIN lock and keep default security controls &measures on device.
Cyber incident response plan	This should address mitigation and isolation of affected systems, cleanup and minimizing loss of information.

Source: Author's processing based on Mitre.org

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-8-6/July 2022

5. Conclusions

The specific field of malware detection and prevention for internet banking is in its first years of development. On the one hand taking into account the recent increase in usage of internet banking by customers and on the other hand because of increased regulatory requirements for payment service providers in this respect. Information about potential threat is available more, either publicly available (free of charge) or in the form of threat intelligence offered by specific vendors (and/or public authorities). Given the specifics of the internet banking applications, there are specific malware that are used in this respect and not general malware. According to the data available, there are only very limited situations in which the operating systems of mobile and other types of devices and the browsers have also taking some security measures for detection and prevention against malware. However, at the same time, such stakeholders have limited the data available for internet banking solution to analyze malware existence on a device by limiting the access to various data sources on the device.

In such a context, given the large amount of data on malware and the limited mechanisms of detecting and preventing malware when internet banking is used on user devices. The mechanisms for prevention are limited, given the fact that the device is owned and handled by the user and out of the control of the payment service provider. In this case, the measures that the payment service provider can take are at the level of the internet banking front-end web / mobile application or at the level of the back-end thereof. As detailed in this research paper, there are certain criteria that can be taken into account when addressing the prevention of malware when internet banking is installed on user devices and when it is used. The criteria we have built on in this research paper have multiple sources and focus on the Mitre information, as this includes a significant amount of data about malware, including banking malware. Certain types of cyber-attack techniques and resulting vulnerabilities can be addressed by the payment service provider (with the use of little or a large amount of resources – costs and effort), while others cannot be addressed but only have implemented detection techniques in order to refuse payment in the case of malware presence. In such case, the process has to include notifying the customer about the malware presence. For this reason a risk-based approach is presented in this research paper. Further research on this topic can build on the above framework and extend it in terms of criteria to be included in the risk-based approach and in terms of the level of risk for each vulnerability identified.

Author Contributions: Conceptualization, M.C.S., L.G., L.A. and C.N.B.; Methodology, M.C.S., L.G. and I.B.; Formal analysis, L.G., I.B., L.A. and C.N.B.; Investigation, M.C.S., L.G., L.A. and C.N.B..; Resources, I.B L.A. and C.N.B.; Data curation and analysis, I.B. and L.G.; Writing—original draft preparation, L.G., I.B. L.A. and C.N.B.; Writing— review and editing, M.C.S., L.G., I.B. L.A. and C.N.B.; Visualization, M.C.S., L.G., I.B., L.A. and C.N.B.; Supervision, M.C.S.; Project administration, M.C.S.; Funding acquisition, M.C.S and I.B.

All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by a grant from the Romanian Ministry of Education and Research, CNCS-UEFISCDI, project number PN-III-P4-ID-PCE-2020-2174, within PNCDI III.

Data Availability Statement: Data used in this analysis is not public, but available upon request.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

Abdullah, R. M., Abualkishik, A. Z., Isaacc, N. M., Alwan, A. A., Gulzar, Y. (2022). An investigation study for risk calculation of security vulnerabilities on android applications. *Indonesian Journal of Electrical Engineering and Computer Science, Vol. 25, No. 3,* 1736-1748.

Achim, M. V., Borlea, S. N., & Văidean, V. L. (2021). Does technology matter for combating economic and financial crime? A panel data study. *Technological and Economic Development of Economy*, *27*(1), 223-261.

Achim, M. V., & Borlea, N. S. (2020). *Economic and financial crime. Corruption, shadow economy and money laundering.* Springer Nature Switzerland AG.

Adam, M., Soliman, A. M., Mahtab, N. (2021). Measuring enterprise risk management implementation: A multifaceted approach for the banking sector. *The Quarterly Review of Economics and Finance (e-journal),* vol. 84. Available at: <https://doi.org/10.1016/j.qref.2021.01.002> [Accessed on May 2022].

Amankwah-Amoah, J., Khan, Z., Wood, G., Knight, G. (2021). COVID-19 and digitalization: The great acceleration. *Journal of Business Research, 136,* 602-611.

Black, P., Opacki, J. (2016). Anti-Analysis Trends in Banking Malware. *11th International Conference on Malicious and Unwanted Software (MALWARE)*, 1-7.

Chaudhary, V., Mandaviya, M., Sameen, H. S., Manoor, J. P., Bharti, A. (2021). A study on effect of various demographic factors on preference of consumers towards online banking usage. *Materials Today: Proceedings.*

CISA Review Manual 27th Edition (2019). Available at: < https://dokumen.pub/cisa-review-manual-27th-edition-1604207671-978-1604207675.html> [Accessed on May 2022]

Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (2018). Available at: < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389> [Accessed on May 2022]

Eurostat. (2021). Individuals using the internet for internet banking (dataset). Available at: <https://ec.europa.eu/eurostat/web/products-datasets/-/tin00099> [Accessed on May 2022]

Haidar, N. S., Almustafa, M. M. (2022). E-banking Information Security Risks Analysis Based on Ontology. *International Journal of Science and Innovative Research,* 02(08).

Hayikader, S., Abd Hadi, F. N. H., Ibrahim, J. (2016). Issues and Security Measures of Mobile Banking Apps, *International Journal of Scientific and Research Publications*, *Vol. 6*, Issue 1.

Jebarajakirthy, C., Shankar, A. (2021). Impact of online convenience on mobile banking adoption intention: A moderated mediation approach. *Journal of Retailing and Consumer Services, vol. 58*, no. 102323.

Kadir, A. F. A., Stakhanova, N., Ghorbani, A. A. (2018). Understanding Android Financial Malware Attacks: Taxonomy, Characterization, and Challenges. *Journal of Cyber Security and Mobility, Vol. 7_3*, 1–52.

Kumar, K. A., Raman, A., Gupta, C., Pillai, R. R. (2020). The Recent Trends in Malware Evolution, Detection and Analysis for Android Devices. *Journal of Engineering Science and Technology Review, no. 13 (4),* 240 – 248.

Mira, F. (2020). An overview of the detection of malware, tools and techniques. Waffen-und Kostumkunde Journal, Available online at: <https://www.druckhaus-hofmann.de/gallery/10-wj-march-2162.pdf> [Accessed on April 2022].

Mitre (2022). Available at: < https://www.mitre.org/> [Accessed on May 2022]

Mobile Banking Risk Identification and Mitigation (2014). Community Banking Connections: A Supervision and regulation resource. Available at: <https://communitybankingconnections.org/articles/2014/q1/mobile-banking-risk-identification-and-mitigation> [Accessed on May 2022]

More, M. M., Jadhav, M., Nalawade, K. (2016). Online Banking and Cyber Attacks: The Current Scenario. *International Journal of Advanced Research in Computer Science and Software Engineering, 5(12).*

Robertson, D. (2016). *The Nilson report*. Available at https://www.nilsonreport.com/upload/content_

promo/The_Nilson_Report_10-17-2016.pdf. Accessed on 21th March 2022.

Ryman-Tubb, N. F., Krause, P., & Garn, W. (2018). How Artificial Intelligence and machine learning research impacts payment, card fraud detection: A survey and industry benchmark. *Engineering Applications of Artificial Intelligence, 76*, 130–157.

Sachdeva, S., Jolivot, R., Choensawat, W. (2018). Android Malware Classification based on Mobile Security Framework. IAENG International Journal of Computer Science, 45:4.

Șcheau, M.C., Gaftea, V.N., Achim, M.V. and Bodescu Cotoc, C.N. (2020) Cyber Security Reactivity in Crisis Times and Critical Infrastructures, 24th International Conference on System Theory, Control and Computing (ICSTCC), pp. 691-698, doi: 10.1109/ICSTCC50638.2020.9259695.

Shankar, A., Rishi, B. (2020). Convenience matter in mobile banking adoption intention? *Australasian Marketing Journal (AMJ), Volume 28, Issue 4*, 273-285.

Statista (2020[1]). Development of new Android malware worldwide from June 2016 to March 2020 (in millions). Available at: <https://www.statista.com/statistics/680705/global-android-malware-volume/> [Accessed on May 2022]

Statista (2020[2]). Countries most targeted by banking malware attacks in 2020. Available at: < https://www.statista.com/statistics/325226/countries-by-users-attacked-by-financial-malware/> [Accessed on May 2022]

Statista (2021). Most prevalent banking trojans worldwide in 2020, by type. Available at: < https://www.statista.com/statistics/1238991/top-banking-trojans-worldwide/> [Accessed on May 2022]

The Financial Task Force (FATF) (2014). Guidance for a risk-based approach. The banking sector. Available at: <https://www.fatf-gafi.org/documents/riskbasedapproach/documents/risk-based-approach-banking-sector.html?hf=10&b=0&s=desc(fatf_releasedate)> [Accessed on June 2022].

VosViewer (2022). Version 1.6.18. Available at: <https://www.vosviewer.com/> [Accessed on March 2022].

Windasari, N. A., Kusumawati, N., Larasati, N., Amelia, R. P. (2022). Digital-only banking experience: Insights from gen Y and gen Z. *Journal of Innovation & Knowledge*, *vol. 7*, no. 100170.

Yoo, S., Ryu, H. R., Yeon, H., Kwon, T., Jang, Y. (2019). Visual analytics and visualization for android security risk. *Journal of Computer Languages, Vol. 53*, 9–21.