PRIVACY AND SECURITY CONFERENCE 2021

PRIVACYANDSECURITYCONFERENCE.PT

Proceedings of the Digital Privacy and Security Conference 2021

20 - 21 January 2021 *Porto, Portugal*

Editors
Carla Cordeiro and Hugo Barbosa

UNIVERSIDADE LUSÓFONA DO PORTO

Copyright

1st Edition 2021

Issue EOI:10.11228/dpsc.03.01

Editors: Carla Cordeiro and Hugo Barbosa

Proceedings Design: Hugo Barbosa

Graphical Design/Website: Hugo Barbosa

E-mail: hugo.barbosa@ulp.pt

Conference Website: https://privacyandsecurityconference.pt

Conference EOI :10.11228/dpsc

DPSC2021 Proceedings EOI: http://eoi.citefactor.org/10.11228/dpsc

Universidade Lusófona do Porto
Rua Augusto Rosa, nº 24
4000-098 Porto – Portugal
Telephone: +351 222 073 230

FOREWORD

ORGANIZING AND SCIENTIFIC COMMITTEES

Digital Privacy and Security Conference 2021 Organization and Scientific Committees welcome you to the fourth edition conference.

In times of pandemic, we live very difficult times, but also of learning and growth as a society, together we will be able to overcome. The Organizing Committees of the DPSC2021 Conference have worked hard behind the scenes to make the 2021 edition safe and successful, considering that COVID-19 is an extraordinary global public health problem. The Digital Privacy and Security Conference 2021(DPSC2021) is ON and will be ONLINE only in this edition.

The main goal of a scientific event is to discuss, disseminate and create knowledge. Organizing this conference proved to be a challenging opportunity for us to achieve this goal.

Currently, we are living in a digital world, where we share all information consciously and subconsciously about our life with any one. This situation puts the people in a worrying situation. Areas such as industry, health, finance, among others are addressed at the conference taking into account the problems of each sector. Our commitment and hard work have as aims to contribute for all participants to acquire tools to better protect themselves. This area is in constant evolution and need we improved our knowledge.

The young students that devote themselves to research deserve our praise for their efforts in the search of new knowledge and better intellectual and technical skills. Persistence and strong motivation constitute the driving force which stimulates students of Security and Audit class the Informatics Engineering degree from the Lusofona University of Porto (ULP), to the creation of scientific papers related to this field of study, to the promotion of research, and to the knowledgeable discussion and practical demonstration on a variety of issues addressed, particularly in the context of computer science, computer networks and computer forensics. The grouping of this information,

which takes the shape of a book, is the natural result of these principles put into practice.

We would like to thank all those authors whose participation in this endeavor contributed to its success, hoping it will promote a better understanding of the issues that were addressed. A special thanks to all the members of the scientific committee who, with their contribution, allowed to raise the level of the conference.

Thanks to all the sponsors who made the conference possible, as well as all those who contributed to the success of DPSC2021.

Porto, January 2021

Carla Cordeiro and Hugo Barbosa

Conference Committees

Organizing Committee

Carla Moreira Cordeiro – Universidade Lusófona do Porto, Portugal
Lusofona University of Porto, Portugal

Hugo Azevedo Barbosa – Universidade Lusófona do Porto, Portugal
Lusofona University of Porto, Portugal

Scientific Committees

Hugo Azevedo Barbosa - Chair
(Lusofona University of Porto, Portugal)

Óscar Ferreira Ribeiro
(Lusofona University of Porto, Portugal)

José Lobinho Gomes
(Lusofona University of Porto, Portugal)

João Ulisses
(University of Vigo, Spain)

Günther Pernul
(University of Regensburg, Germany)

João Paulo Magalhães
(ESTG - Polytechnic Institute of Porto, Portugal)

Kiavash Satvat
(University of Illinois at Chicago, United States)

Esma Aïmeur
(University of Montreal, Canada)

Weizhi Meng
(Technical University of Denmark, Denmark)

Support Committee

Catarina Freitas (EPCJC, Portugal)

Cíntia Torres (EPCJC, Portugal)

Maria Oliveira (EPCJC, Portugal)

Sandro Moreira (The Fleet Kollective, Portugal)

Sponsors

Institutional Partners

ORDEM DOS ENGENHEIROS REGIÃO NORTE

Sponsors

Media Partner

Contents

SESSION 1 - Privacy and Security in the Era of Digital

SESSION 2 - The Future of Risk Management in the Digital Technologies

SESSION 1
PRIVACY AND SECURITY IN THE ERA OF DIGITAL

The Security of Portugal Smart Cities: Vulnerabilities, Risks and Prevention

Gabriel Lima

University Lusófona from Porto, Portugal

gabrielfariali@hotmail.com

Abstract. In the current age, it is noticeable that the evolution of modern society leans towards faster and simpler ways of doing any type of daily task, in that sense, it would not be too late to introduce the concept of Smart Cities, a city with improved networks and services like public transport, water storage, light, and efficient administrative services are optimal as possible with the use of digital and telecommunications technologies for the benefit of its inhabitants and internal businesses. But smart cities are quite a double-edged sword topic as they can provide effective and efficient delivery of services, yet they can create new vulnerabilities and threats, possibly making the city insecure and open to several forms of criminal activity. In this study, we aim to examine this technology in Portugal and go deeper into this mostly forgotten topic about the insecurities concerning smart cities, specifying the risks that the country can currently face due to not considering security tests of new technologies and not granting the full protection of this huge communication. In the common sense that any city can start investing in this kind of environment, is only logical that the security has to be directly proportional in terms of investment, in this sense this paper also aims to expose existing forms of strategies to prevent (Strategies like awareness regarding cybercrimes is pivotal for tackling and preventing cybercrimes, factors such as social media, government initiative and organizations play a huge role in preventing any of these cybercrimes) or deal (formation of core security and computer emergency response teams, a change in procurement procedures, and continuing professional development) with any type of security tribulation.

Keywords: Portugal, Cyberattack, Risk, Security, Smart Cities, Urban Resilience, Prevention, Vulnerabilities, Social Engineering, Digital Services.

1 Introduction

The concept of the "smart city" has experienced a considerable increase in studies and analyses in academic or industrial fields. The promise of solving and optimizing everyday problems encourages cities to take an interest in this new type of environment. According to a study by United Nations in 2014, more than half of the world's population now lives in urban areas, and the trend is rising, with forecasts for 2050 already at around approximately 66% [1]. These data do not differ from what is currently happening in Portugal, where the number of people living in urban areas is gradually and continuously increasing [2], as shown in these United Nations graphs.

10.11228/dpsc.03.01.001

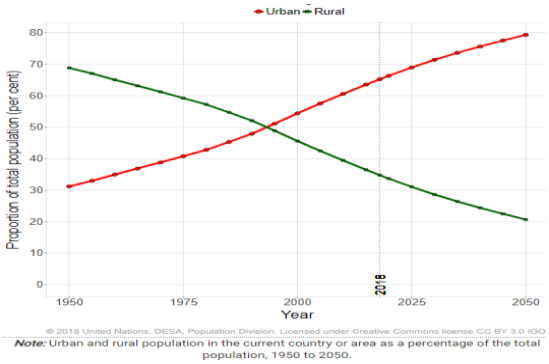


Fig. 1. Percentage of population in urban and rural areas in Portugal.

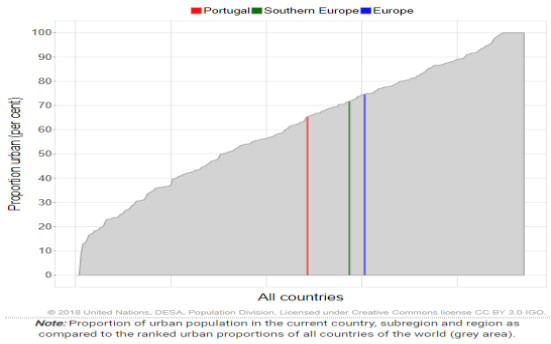


Fig.2 Percentage urban by country in 2018.

This population increase certainly brings with it new social challenges, such as the inability to provide the entire population with the necessary supplies, increased waste, and, as a result, flooding, or health problems. The problems certainly even affect the environment around an inhabited city [3]. Just as urban population growth, developments in the world of technology have not stopped growing, it did not take long for the idea of a technology network to emerge that can provide effective, rapid, and practical solutions for managing any area where this is required, so a "smart city" emerges when a deficiency or insecurity in the social sphere is effectively addressed, with the aim of alleviating the challenges and improving the well-being of a citizen; in addition to addressing current problems, a smart city has an incredible potential for expansion and can intelligently support economic, environmental and social developments. Following the same line of thought, one can imagine the creation of many new, "smart" ways of tackling everyday problems, such as a smart transport system, a smart government system, a smart health system, a smart environment system, a smart transport system or even smart houses and buildings. According to IDC, investment in smart city initiatives is growing exponentially [4], and we can imagine why hundreds of cities are interested in such an effective tool for urban development and management.

1.1 Paradox in smart cities.

Like any kind of new technology, the promises of utility and exclusivity is always of enormous interest to the large population, the same, many times is not interested in the in-depth analysis of new technology and not realize what it can accept in your personal life. The process of adapting to a new technology brings with it a series of innumerable problems related to security, even more so when this technology is a complicated architecture of networks and intelligent systems that can and should involve an entire city, there are frequent attacks on intelligent systems on a daily basis, such as unauthorized access or denial of service (Dos). Since the attempt to build an intelligent electricity system, there have been unprecedented attacks, such as the failure of the power supply in Ukraine in 2015 due to hacker attacks [5], cases of excessive data collection by service providers that pose a threat to privacy [6], or Russian attacks on the US electricity system. In discussing the term cyber-attacks, the energy secretary Rick Perry says that "literally hundreds of thousands of times a day" [7 . Such a statement puts into perspective the great para-doxia of smart cities, a promising and visionary environment in which problems with energy, transportation, water, or government administration can be solved as simply and easily as possible, but few analyze or worry about the great security risk associated with such a system.

There is a fine line between promoting the well-being of society through technology and opening up new risks and vulnerabilities for it. This paper attempts to explore this relationship between risks and benefits by examining the already documented and observed risks posed by this system, attaching importance to the extent of vulnerabilities that allow threats to violate and denigrate the level of integrity, confidentiality, and availability of the system, and also looking at the preventions that can be taken in the search for a safer future. all these topics will be covered below in Chapters 2 and 3.

2 Risks and Vulnerabilities of Smart City

A critical analysis of the history of mankind shows us an important fact: with the constant progress of technology, some seek or simply find ways to attack, penetrate, corrupt, or cheat the virtual environment. These attacks can be the fruit of malicious intent with some kind of personal interest or oversight that was carried out without any idea of possible subsequent events [8]. Smart Cities are no different from these because the size of their system covers a surprising range of vulnerabilities and risks; the most promising problems of a smart city are related to a system failure due to attacks or malfunctioning of the system, or to a large scale data breach [9]; it is noteworthy that this type of system combines several characteristics that make it vulnerable, the process of centralization and integration of technologies, coupled with a full Internet connexion, makes this system a major potential target for attackers who could access this network and cause damage on a large scale. One factor that should be noted is the fact that Ukraine has in the past experienced terrible episodes of total power loss [5]. It is inevitable to make a comparison that an attack of this magnitude was not possible in ancient times, and we can still say that we are increasingly moving towards having vital infrastructures in our society that are potentially vulnerable to a series of new attacks, even

worse given the fact that, because of the time we live in, these attacks can be commanded by people all over the world, as was the case with the Russian cyber-attacks on the United States, which were also mentioned earlier. All these attacks are living proof of the risks to which we are exposed as a society, bearing in mind that the introduction of an intelligent system is inevitable over the years, which demonstrates, even more, how important analyses, studies, preventive measures, and the whole process of cybersecurity are today and even more so in our daily lives.

According to Shirey and the Internet Security Glossary, the threats that a system can face are divided into four categories: Attack on the correct operation of a system (disruption), inducing error (deception), unauthorized access to information (disclosure), and usurpation [10]. These categories can be characterized as follows [11]:

- Disruption is defined by the corruption or degradation of systems that have a negative impact on the services offered; this situation usually occurs when the system component to which the information is delivered is directly disabled or when the system is requested to transmit contaminated data.
- Deception is described by the deliberate effort to deceive different entities. For example, a vengeful entity may send false or inaccurate data to another person in the belief that the data is correct. Fake entities can be used to incriminate others or gain unlawful access.
- Disclosure is characterized as gaining unauthorized access to secure data. Delicate information could be wrongly presented to unauthorized elements or could be obtained by an attacker who circumvents the security precautions of the framework.
- By usurpation an attacker can gain unauthorized control over a system. This unauthorized control may allow the attacker to illegally gain access to secured information or services or to disrupt the framework itself to cause false or malicious behavior.

It is also important to identify that the vulnerabilities of a system are usually originated by common and major failures, such as:

- Poor design: Systems are created with security holes.
- Poor implementation: Systems are incorrectly configured and therefore vulnerable to attacks.
- Poor management: The testing procedures are inadequate, or insufficient or both. Security measures may not have the support, documentation and monitoring necessary for the correct functioning of the system.
- Physical means: The physical installation is not adequate and consequently the physical protection of equipment is compromised, every system is vulnerable to unforeseen situations and human failures and these can range from sloppiness, laziness to greed or some personal revolt.

In this paper we try to highlight the two main risk areas in a Smart City, focusing on attacks that directly affect system availability, integrity and also confidentiality.

2.1 Attacks on confidentiality level, Data Breaches

The nature of a smart city is the connection of objects present in your network to provide continuous communication and dynamic services, this interconnection is ensured through various objects and in various areas in our daily lives, we can cite as an example the so present Embedded System such as smartphones, TVs, printers or as many other specific engineering devices. Besides common embedded systems, there is a range of objects that are not taken into account such as clocks, household appliances, sensors that can be used to monitor any type of information desired, doors, bridges for education. In this way Smart cities are directly involved in data collection, intensive analysis, and storage of tons and tons of data each one of them related to an entity of the society, information that is sensitive and valuable that we almost never realize of yielding to a platform of the government, what can happen as well is the very terms of conditions request the freedom to be as evasive as they want like sharing the data with danger third parties if the user allows it unnoticed.

We can adopt an even more pessimistic view of the scenario, an intelligent system that could monitor each of an individual's actions, storing and analyzing data to build a profile linked to them. If this profile, loaded with sensitive information, is in some way intentionally or unintentionally leaked or stolen due to some exploitation of the vulnerabilities and risks of the system, this would pose an unprecedented threat to the individual in question. The attacker could then have access to the individual's location and monitor each of his or her steps, knowing the right times to commit robbery or even assault against the individual. Furthermore, we are still at risk of being the target of a deception attack, that is, the attacker uses the data in an unauthorized way to steal the information he wants, it is possible to realize that the information leads to knowledge and the knowledge leads to power, that is, by obtaining this data, an attacker has countless ways of taking advantage of it and benefiting himself consequently affecting those who own the data.

According to DLA Piper survey, in Europe over 59,000 personal data breaches were reported [12], and the International Data Corporation predicts that by 2020, a quarter of the world’s population will have been affected by a data breach [13]. In Portugal we have reports and analyses according to the International Network of Privacy Law Professionals that show a severe lack of concern with the information collected [14], resulting in fines that will need to be paid to GDPR.

Despite the great risks involved in data collection, one thing is certain, the analysis and collection of this information will allow the emergence of an intelligent model that can deliver all the intended benefits. Even in a non-smart city environment, where many Portuguese citizens use their smartphones for trivial things like checking the climate, they are benefiting from this vast network of data collection, The purpose of this paper is not to condemn this practice, which has already been adopted, because it would be impossible, but to focus on imposing limits when a data collection is something profitable and good for the urban development of all or when a collection is compulsive and

directly affects the most valuable asset of society, namely its own people, whose privileges are attacked and whose identities are stolen in exchange for a set of data. This kind of practice can evolve even more if we think of a world where all the data we use is organized and archived, this betrays a huge policy of fear of the people in relation to the government, where the government could have all the knowledge possible and consequently manipulate the mass for its own benefit without it noticing it, while the people would know the minimum due to the lack of transparency of the system, as a final result democracy itself and individual freedom of choice could be affected directly with the excessive date breach as we can see current examples such as [15] and [16] where many of the technologies that are frequently associated with smart cities have been used to create a surveillance state, where the people can no longer practice their religion openly or assert the individual freedoms that we take for granted.

A complete survey [17] suggested that four sources of facts can be used to hack privacy, namely, observable data, repurposed data, published data, and leaked data, which carries a giant quantity of users' touchy information. Sometimes, the privateness of residents can be breached even although a device is tightly closed and not harmed through offenders. One practicable way for this to occur is the effective data mining algorithms. With these mining tools, some service providers and third events can easily discover consumers' private information, for example, the example provided by [18]. Besides this tool, we also have an attack to which we are all exposed, the attacks of social engineering. These attacks correspond to a large part of the threat and risk to smart cities, both in data breaches and attacks against the availability of the system. The criminals who use this technique try to deceive the user so that they can perform actions that will cause great failures in the information security system, the damages, and causes of this strategy can vary according to the profile of the attacker and his objective, it can be just a form of trot to get sensitive data in an easy way or assuming an extremely greater magnitude with the possible corruption and disruption of public transportation systems, so it is possible to cause serious accidents, the city's water system could be damaged, as well as its nuclear plants or any other type of installation that will always be of extreme importance for the social good of the population. A common and long-standing form of attack on the system's confidentiality using social engineering resources would be phishing attacks, which means, targeting email users to capture the user's credentials. Hackers can use the information gained to access smart city systems for malicious purposes. The techniques and technologies behind phishing will continue to evolve [19]. The graphic below shows the number of data breaches in Europe according to [12] and we can see how Portugal is dealing with the situation in data breaches in relation to other neighboring countries, taking into account that the population difference plays a big role in a possible comparison of situations.

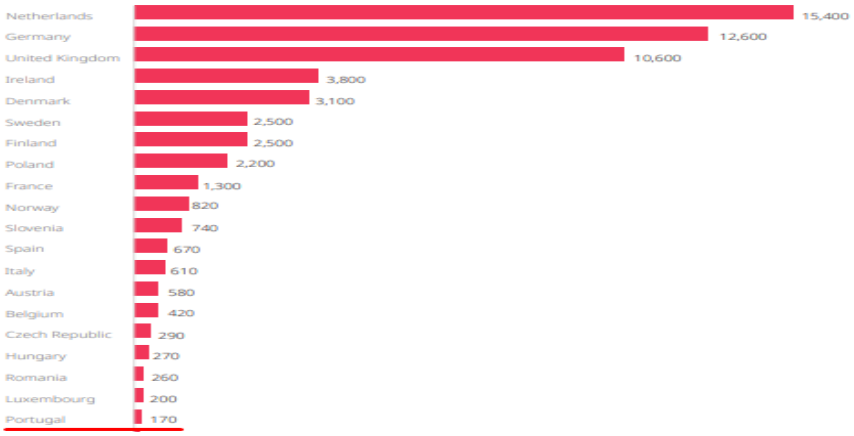


Fig. 3. Number of data breaches notified from May 25,2018 to January 28,2019

2.2 Attacks on Availability and integrity level

The most effective way to compromise the complex network of a smart city is through cyber-attacks that seek [19]. As soon as a device is compromised as a result of an attack, its whole set becomes vulnerable for any type of next attempt, these compromises or cyber-attacks are imminent threats to any type of smart city, as already discussed there are a series of risks and vulnerabilities to be exploited by attackers, one of these threats that would seek to interrupt the correct functioning of a system, denying its service of use to the population would be threats against the vulnerable points of the SCADA (Supervisory control and data acquisition) system.

SCADA. It is a system that controls functions and workflows of various urban infrastructures, we can highlight the electrics grid, water supply, and traffic control, all these rely on real-time analysis that the SCADA system provides in addition to automated services for changing settings in your system, requiring human intervention only in special cases. It is expected that a system of such importance in the daily life of any smart city will have to be well protected for the good of the population, in practice what we find is that supervisory systems of control and data acquisition can be tracked since the year 1920 [20] and as consequence many of these systems are now outdated in the face of the reality of computer evolution and consequently the evolution of cyber-attacks.

Severe SCADA systems have already been compromised, [8], [20], [25],[28] where their attackers alter the performance of urban structures and cause the population to cease using the service. In 2014 a study [21] showed that out of a total of 599 security executives from utility, oil and gas, energy and manufacturing companies, almost 70% recorded at least one security breach that led to the disruption of the performance of these infrastructures, moreover when asked about the probability of future attacks on ICS organizations or SCADAS systems, 78% of state security officials say that a

successful attack on the security of organizations is expected in the next two. These studies are frightening news given that these industries play a large role in a global economy and could in no way be such easy targets for an attack to degrade the system.

There are infrastructures that will certainly have more impact when compromised by some kind of attack, we can cite two very important ones that would be the electric network of a city and the management system of transport and vehicles.

Attacks on the electricity grid. Events of attacks against the availability of electricity grids around the world [5], [7] have already been discussed in this paper; these grids use the SCADA system to generate, transmit and distribute electricity in a monitored and controlled manner [20], and are therefore a major target for attackers because of the magnitude of services this infrastructure provides to the population of a city. These power grids have been present for a long time in large spots, so it is not strange to hide outdated systems in their security and prevention levels, so the current level of daily attacks on power grids increases considerably [20] and ways are increasingly being found to compromise all this infrastructure with low-cost tools [22], [23] increasing the fear of a "smart" future.

Attacks on Transport management systems and vehicles. Just like electricity networks, attacks against the transportation management system are also extremely common and this tendency to attack continues to increase with the arrival of new attackers and new discoveries made by them, so studies and news also emerge frightening in relation to existing attacks and concerns, we have as example situations where attackers managed to stop the main street for 8 hours causing a great disturbance in traffic [24]. Like any technology, these cyber-attacks also seek to evolve and learn the most realistic and effective way possible in their attacks, so we can have access to studies that show hundreds of traffic lights having their service of use denied by just a laptop and a wireless radio [25], there are already cases that stir up the fear of an attacker being able to attack a system from anywhere in the world [26] or cases where passengers on the edge of a train were injured due to a breach of security made by a teenager [23], [27]. But these attacks are not only exclusive to public transportation in a city, any vehicle today also has total vulnerability to some kind of disruption to its system, as we know a modern car can contain numerous sensors connected to various control units that in turn connect to wireless networks.

It has already been observed attackers taking advantage of this knowledge [28], taking control of the entire internal computer network of a vehicle, being able even to cut the physical control of the citizen in his own car and assuming it remotely and completely, thus being able to practice any act of evil against the individual attacked.

3 Possible preventions

A common factor observed in history is that since the appearance of belongings and interests, those who are in charge of identifying and exposing vulnerabilities to

get these interests also appear. With all the time any kind of security, sophisticated or innovative will inevitably be the target of a defeat against a determined attacker, every security system already starts from an evident disadvantage knowing that the main advantage of the attacker is that he only needs to find a single weakness, while the administrator must find and eliminate all the weak points to achieve perfect security, it is thus given the need to adopt certain practices in search of mitigations and controls throughout this gloomy scenario presented.

Two types of key risks need some mitigation process, one would be the process of ensuring a good design and a good implementation of the system, with new technologies that are implemented in this vast network or possible "smart" upgrades to existing urban infrastructures, and the second would be the process of mitigation of data generated, stored and shared through this vast network, i.e. data breaches.

When we analyze the means of mitigation, we can see that they can arise from two main points, they can be measures adopted in the scope of the market presence in the system or they can be measures adopted in the scope of the government itself as an entity that has powers, rights, and duties and also seeks to mitigate as much as possible any adverse situation to the welfare of society.

As discussed previously in the two key types of risk and also the most common origins of vulnerabilities in a system, an approach made at the level of the market of a smart city has to start from security by design, with each new implementation of a smart city system it is necessary to guarantee levels of protection to preserve the well-being of the society, these levels refer to:

- Transparency with citizens
- Accountability
- Anonymity and security measures
- Cyber defense services appropriate and always updated
- Standards, practices and regulations of safety and use

Making this practice something immutable over the years, software companies could then help each other with the creation of thorough and rigorous standards in the area of security, as well as the creation of good practices that could thus put the team of defense against cyber-attacks in a fair fight with the incredible evolution of the means of attack over the years, after all, the best way to prevent risks from happening is not to create vulnerabilities in the first place.

With this kind of thinking where each company practices constant self-evaluation and also encourages others to do the same, security becomes more and more necessary and of fundamental importance in any new addition to the great network system in a smart city, making companies that don't adopt this method look bad in the public eye, bringing a competition that any business wouldn't want to be behind.

The measures adopted by the government should also always seek to guarantee the levels of quality in protection, an example of a measure to be adopted and perhaps the most important in the field of data breaches would be information open to all citizens of a smart site about how data collections happen and how they are used, a transparent system will always bring more comfort and security. The best possible scenario for a citizen would be the personalized privacy of their data in the best

possible way and still be possible the effective use of the functionalities of a smart city and this is the thinking that would replace the current thinking of the bigger the data collection the better [29]. Mitigations methods are not complete without a damage assessment plan, any system is subject to attacks so every system must be equipped with maneuvers to minimize the damage that has occurred, a zeal for data begins with storing it on various platforms and "safes" capable of storing the information in cyclical periods and can serve as the decisive tool for data recovery when needed.

Even the best mitigation strategy and effective prevention would not be able to eliminate all the vulnerabilities and risks associated with a smart city environment, in the search for the evolution of security, several mechanisms were developed to protect the levels of availability, integrity, and confidentiality of the systems but in the direct application of these mechanisms there were always failures, This is due to the same reasons of prevention in marketing levels, the mechanisms launched do not pass through any standard of quality customized for the environment of a smart city, such as the numerous sensors scattered in this system do not have the processing power necessary to accommodate high-end security mechanisms and because of this can only be configured with weak encryption systems being a huge risk for the entire structure.

Currently, all new mechanisms intend to follow the trend line of the new technologies, that is, they need to be more and more practical, flexible, dynamic, and low cost for the mass acquisition by some entity, the concern and the best investment in this current framework would be the deeper research in ways to guarantee all these qualities to the simplest sensor, while the necessary levels of protection are guaranteed, beating against security by design being one of the best practices to adopt.

Unfortunately, according to the current picture, the threats faced and the future fears it is fair to conclude that more effective forms of protection, prevention, and mitigation need to be developed to keep pace with the great growth of attacks and the "smart city" concept, this kind of thinking where security has its place is the best chance of new opportunities and new frameworks within such a huge and dangerous technological environment.

4 Conclusion

In this paper we can go deeper into the current state of security in a smart city environment in Portugal, we can clearly analyze the duality of this system that promotes a basis for the creation of a new social architecture allowing environments that support an undefended number of computer protocols occur simultaneously for the welfare of society, despite the benefits that smart cities bring, also create new risks and in unimaginable degrees opening up forms of vandalism, disruption, and criminal exploitation.

It is noticeable how the development of new methods and models of protection is essential and in great demand, because it is a challenge of magnitude above the communitarian, and because of that this paper also seeks to discuss the current problems in companies and in bigger entities like the government about new approaches and

strategies of adoption benefitting the general welfare such as security-by-design and the continuous improvement from the adoption of the protocols of good practices being done by all the elements that compose this system, This adoption process should be taken with a regulatory approach for entities that have a higher risk and consequently higher side effects involved with their system, thus being able to be transparently monitored to the public and guaranteed compliance with the suggested standards.

Evidently we cannot stop the evolution process that directs these systems, but it is not yet late to analyze how we will make this transition and how we will ensure total control and use of it, currently, values are inverted and not given due importance to issues that really matter such as the extent of security and vulnerabilities.

With the forms of prevention discussed in-depth and maneuvers that would promote an incredible advance in the current situation, it is possible to have smart cities that only offer optimized services and a better quality of life without the blatant concern of the greatest risks of privacy and security, as long as more and more importance is given to the security and privacy of the citizens, with the several rigorous criteria being applied to each stage of the development of a system of this magnitude, it is possible to believe that someday we will have this new help that technology would bring to the daily life of each one of us, in the current and future days.

References

1. U. Nations, “World urbanization prospects: The 2014 revision, highlights. Department of economic and social affairs,” Population Division, United Nations, 2014.
2. Macrotrends Portugal Urban Population Page, https://www.macrotrends.net/countries/PRT/portugal/urban-population, 2018, last accessed 2020/11/22
3. National Geographic urban threats, https://www.nationalgeographic.com/environment/habitats/urban-threats/, 2020, last accessed 2020/11/22
4. IDC’s Worldwide Smart Cities Spending Guide page, https://www.idc.com/getdoc.jsp?containerId=prUS46016320,2020, last accessed 2020/11/22.
5. Author, F.: Contribution title. In: 9th International Proceedings on Proceedings, pp. 1–2. Publisher, Location (2010).
6. Humans Rights Watch, “How Mass Surveillance Works in Xinjiang, China”, https://www.hrw.org/video-photos/interactive/2019/05/02/china-how-mass-surveillance-works-xinjiang, 2019, last accessed 2016/11/21.
7. Rick perry, “Energy and water development appropriations for 2019”,https://www.govinfo.gov/content/pkg/CHRG-115hhrg32414/pdf/CHRG-115hhrg32414.pdf, 2019, pp 140, , last accessed 2021/01/12.
8. NATO review magazine “The history of cyber attacks – a timeline”, https://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm, 2013, last accessed 2020/11/24
9. Josh Lake, Comparitech “Smart Cities, Cybersecurity and privacy: What are the risks”, 2019
10. Shirey R RFC 2828: Internet Security Glossary, http://www.ietf.org/rfc/rfc2828.txt, 2000, last accessed 2020/11/22
11. Journal of Internet Services and Applications, “Virtual network security: threats, countermeasures, and challenges”, 2015

12. DLA Piper GDPR data breach survey:, https://www.dlapiper.com/pt/portugal/news/2019/02/dla-piper-gdpr-data-breach-survey/, February 2019, last accessed 2020/11/24
13. International Data Corporation, https://www.csoonline.com/article/3014493/data-breaches-will-affect-14-of-the-worlds-population-by-2020-idc-predicts.html, 2015, last accessed 2020/11/24
14. INPLP, "Portugal: Recent fines for the breach of the GDPR", https://inplp.com/latest-news/article/portugal-recent-fines-for-the-breach-of-the-gdpr/, 2019, last accessed 2020/11/25
15. The new York times, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority", https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html, 2019, last accessed 2020/12/03
16. The new York times, "China Is Detaining Muslims in Vast Numbers. The Goal: 'Transformation.'", https://www.nytimes.com/2018/09/08/world/asia/china-uighur-muslim-detention-camp.html, 2018, last accessed 2020/12/03
17. K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," IEEE, https://ieeexplore.ieee.org/abstract/document/7823349, 2017, last accessed 2021/01/12.
18. L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information security in big data: privacy and data mining," IEEE Access, vol. 2, pp. 1149–1176, https://ieeexplore.ieee.org/abstract/document/6919256, 2014, last accessed 2021/01/12.
19. Oliviah Nelson, Cyber Experts "Smart city security", https://cyberexperts.com/smart-city-security/, 2019, last accessed 2020/12/03
20. The Center for the Study of the Presidency and Congress (2014) Securing the U.S. Electric Grid.WashingtonDC.https://www.markey.senate.gov/imo/media/doc/Markey%20Grid%20Report_05.21.131.pdf, 2013, last accessed 2020/12/05
21. Security Week: "Unisys & Ponemon Institute 2014 Survey".
22. Krebs FBI: Smart Meter Hacks Likely to Spread, April 9th, Krebs on Security, 2012.
23. Nanni, G. Transformational 'smart cities': cyber security and resilience. Symantec, Mountain View, CA, 2013
24. Paganini, P. Israeli Road Control System hacked, caused Traffic jam on Haifa Highway. Hacker News, http://www.markey.senate.gov/imo/media/doc/Markey%20Grid%20Report_05.21.131.pdf, 2013, last accessed 2020/12/06
25. Leitner, T. and Capitanini, L. New Hacking Threat Could Impact Traffic Systems. NBC Chicago, http://www.nbcchicago.com/investigations/series/inside-the-new-hacking-threat/New-Hacking-Threat-Could-Impact-Traffic-Systems-282235431.html, 2014, last accessed 2020/12/06
26. Cerrudo, C. Hacking US (and UK, Australia, France, etc.) Traffic Control Systems, IOActive Blog, http://blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html, April 30th 2014, last accessed 2020/12/06
27. Goodman, M. Future Crimes: A Journey to the Dark Side of Technology – and How to Survive It. Bantam Press, New York, 2015.
28. Greenburg, AHackers Remotely Kill a Jeep on the Highway—With Me in It. Wired 21st July 2015. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, last accessed 2020/12/06
29. K. Xu, Y. Qu, and K. Yang, "A tutorial on the internet of things: From a heterogeneous network integration perspective," IEEE Network, vol. 30, no. 2, pp. 102–108, https://ieeexplore.ieee.org/abstract/document/7437031, 2016, last accessed 2021/01/12.

Data Security and Privacy in Times of Pandemic

David Marques

Lúsofona University of Porto, Portugal
davidmiguelmarques9@gmail.com

Abstract. During what it seems like a big revolution in our lives marked by the presence of this whole new pandemic, each and everyone's life is being put to the test! The covid-19 pandemic had a huge impact in the world and not a single person was able to escape the need to adapt facing this new reality. In continuous and accordingly to what was mention above, this paper will focus on reporting the changes brought by the virus *SARS-CoV-2* into our personal and professional lives. The goal is to emphasize the new lifestyle implemented and the consequences it brought, specifically in terms of the dramatic increase in cyber-attacks.

This paper will be based on real facts in order to contextualize the main theme and it will also put-on display impressive and unbelievable number data registered during this pandemic, focusing on its impact.

The covid-19 rebound in society caused a great threat in the cyber-security levels and for that motive this paper aims to elucidate the importance of good security methods and describes ways and procedures to avoid and react to the majority of cyberattacks that continue to take place during the outbreak of corona virus.

Keywords: Cybersecurity, Security Methods, COVID, Type of attacks during Pandemic, attack prevention

1 Introduction

During this trouble time, cyber security had one of the greatest challenges and it promptly carried out to become the most significant impact in the technological world in the present year. Security in its more informatic meaning was always an essential

10.11228/dpsc.03.01.002

area in the enterprise and companies world, as well as in peoples private lives but due to confinement this topic is now more present in our day-to-day lives than ever.

The goal is to emphasize the new lifestyle implemented and the consequences it brought, specifically in terms of the dramatic increase in cyber-attacks. Sarcastically and with a touch of humour and wordplay we could even say that this new virus allowed a great number of "virus" into our computers. We can surely assume that the pandemic and the lockdown created a huge culture shift in which people have become increasingly relaxed about screen time hours in comparison to life previous to covid-19.

During what seems to be a great revolution in our lives with the presence of this whole new pandemic, the lives of each and every one are being put to the test!

Not only is our health in danger, but also our personal data because during confinement time people spent more hours in front of their computer and the majority of them without any formation in the area. People used computers in order to stay in touch with friends and family but also for work purposes.

This tremendous mobilization to the front of the computer screen, gave the opportunity and the means for those with malicious intensions to launch more cyber-attacks.

With workplaces closed and all the employees working from home in the context of teleworking, the Security department of public companies and big enterprises had to set this operation in a quite rapidly manner by configurating the operations in a remote way. In general, nowadays people are working with unsafe devices which means the hackers can easily get access to companies information. In addition to this, the increased stress felt by the system and the gaps in the collaborative tools intensify the vulnerability to such attacks.

The increase number of cyberattacks happened inevitably because a great amount of companies and organizations didn't have any kind of preparation able to fight off and resist this pandemic. The strategy implemented by these major companies was to simply transport the computers from a safe workplace with the right configuration to their employees personal houses in order to allow them to work safely. Unfortunately, most of the companies focused only on the goal to keep the profit up and keep the work going, they didn't pay attention to the most important factor, the area of security, which has led to the action of several hackers who have managed to obtain much inside information which has put many institutions in danger.

During the course of this year the pandemic challenged, in an unmatched way, the health services and cybersecurity. As result of SARS-COV-2 the number of incidents was the highest ever seen, culminating with the loss of privilege information by several companies, putting them in risk not only in an economical way but also causing mental exhaustion.

Because of everything mentioned above my paper is going to focus on digital security in times of pandemic. It is a very actual theme with a worldwide reach that it is worth discussing in order to improve in the future. To make it more credible I am going to use scientifical references and real-life cases to bring in the humanity factor to highlight the must needed gain of awareness.

10.11228/dpsc.03.01.002

2 Pandemic and impact in world

The covid-19 pandemic had a huge impact in world, and nobody was able to live indifferent to that. The public health consequences of the pandemic have led to a sudden and significant gap in teleworking. Unexpectedly, millions of people and businesses around the world have radically changed their lifestyles by adopting the teleworking regime.

After a few months some people and companies revealed that teleworking was here to stay. We might say that this change brought both advantages and disadvantages.

We will start with the advantages of teleworking, which from a business point of view has reduced operating costs (employee travel, consumption, electricity). The company has achieved exponential environmental gains due to the reduction in traffic and the increase in the number of employees.

On a personal level the advantages of teleworking consist on having facilitated autonomy, flexibility and better work-family reconciliation. The increase in productivity has also been highlighted in analyses as there are no interruptions or distractions that occur while not in the workplace.

Regardless of this, not everything was a sea of roses when it comes to teleworking. The disadvantages began to be revealed as the days were passing and it emerged in an alarming way.

Remote work led to the disappearance of the boundaries between work and family life leading to abusive working hours. Social isolation and individualism at work have occurred in recent months and people have been deprived of face-to-face contact between friends, colleagues and family. This has led to an increase in communication electronics tools such as (Zoom, WhatsApp, Microsoft Teams).

In line with what has been mentioned above and according to what will be addressed more comprehensively in this paper, we will be concluding that the major disadvantage that was brought by this pandemic was in the area of security.

Teleworking has caused thousands of people to start working from home and it has made it easier for them to communicate and for organisations to keep the business going. Unfortunately, it is mandatory to look at the other side of the coin, which refers to the increase number of cyber-attacks. Especially, the remote regime brought more demands for closer monitoring. Like the pandemic if we are not careful, there is a constant exposure. The user, by being unprotected, makes it necessary to be in a constant observation regarding the integrity of the equipment that connects him remotely to the corporate infrastructure.

What happened with teleworking and what was evident in several companies were the vulnerabilities and threats duo to the present situation, which was impossible to predict, appearing unexpectedly. In a way. we can draw a positive balance from this pandemic which has made people more concerned and brought up a number of computer security issues to users and companies.

Organizations have achieved as much as possible in order to have their employees working efficiently from home, but in terms of security the biggest challenge falls on

the employees themselves. They connect to non-secure Wi-fi networks, that most likely have no security measures at all, due to the fact that they probably never give it much thought and it actually makes it easy for the hacker to get on the network.

With several people teleworking and students learning online, this year 2020 has been marked by this pandemic. The confinement and intensity of the news coming to the TV and the excessive research made it difficult for people to distinguish the real from the so famous fake news. As a result, and because of the age we live in, people cling more than ever to the internet as entertainment/leisure and work time, causing Internet traffic to increase intensively.

The security landscape around the world has changed. The COVID-19 effect has been to decree social isolation in several countries in order to mitigate its spread. This adaptation was not guaranteed by many companies because they were not prepared both in terms of equipment and security.

As the days and months went by, it was noted that the gradual increase in contagion from the pandemic led to an exponential increase in malicious activity. Hackers began to take advantage of several people working at home, publishing advertisements in order to deceive users as they worked remotely and began to spend more time connecting to the internet and carrying out activities and looking for information.

Table 1. Most used platforms for attack

Tools	Features	Website
Zoom	Easy to use	https://zoom.us/pt-pt/meetings.html
Google Meet	Secure video meetings	https://meet.google.com/
FaceTime	Best for iPhone, iPad, or other iOS users. The app is only available on the App Store for iPhone and iPad.	https://apps.apple.com/us/app/facetime/id1110145091
WhatsApp	For international chats: Voice and video calls for up to 4 users.	https://web.whatsapp.com/
Google Duo	Best for Android: video calling app	https://duo.google.com/
Skype	No sign ups, downloads.	https://apps.apple.com/us/app/facetime/id1110145091

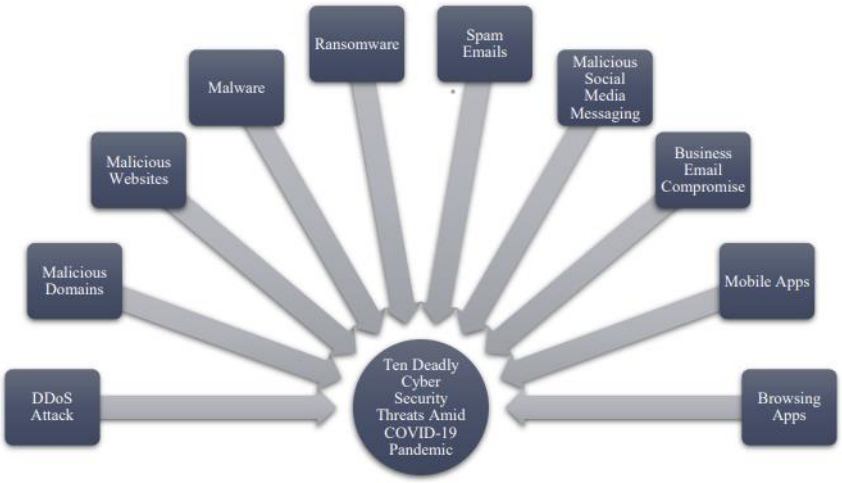
Many students had a great exposure to security due to the need to use tools to hold meetings in a virtual way such as "Microsoft Teams" or "Zoom". The growth of this platform has led to some security problems and cybercriminals have taken advantage of it by creating malicious campaigns. However, it was noted that during this pandemic there was an increase in phishing campaigns as part of Social Engineering.

3 Security Threats

As society has become more and more dependent on technology, it has also become increasingly vulnerable to cybercrime. Cyber security threats are estimated to cost the world $6 trillion a year by 2021, doubling from $3 trillion in 2015[1]. One of the main reasons cybercriminals thrive during pandemics is because heightened emotional states, such as fear, make victims more susceptible to falling into fraud [2]. According to the World Health Organization (WHO), the number of cyber-attacks launched increased fivefold during the COVID-19 pandemic [3]

Since the first cases of COVID-19 in Portugal and the implementation of the new containment measures, there has been an increase in cyber-attacks that use social engineering to take advantage of the fragility of the victims. The most reported attacks during the pandemic were:

Fig. 1. Ten Deadly Cyber Security Threats [5]



3.1 DDOS Attack

Most of the government and healthcare organizations have seen a rapid increase in the Distributed Denial of Services (DDoS) [4]. DDOS attacks are those carried out by cybercriminals against websites or web services, with the aim of stopping them and making them offline. A recent example of this happened when a DDoS attack targeted the

website of the Department of Health and Human Services (DHoS) in the U.S. by flooding millions of users at a time [5].

3.2 Malicious domains

The impact of this pandemic has also caused a lot of fake news and fake applications that circulate through social networks and messaging applications, which only generate disinformation. That is why several major social platforms such as Facebook, Google, LinkedIn, Microsoft, Twitter, Reddit and YouTube have joined forces in the fight against misinformation and the scams surrounding the pandemic. The words "corona-virus," "corona-virus," "covid19," and "COVID-19" have appeared in a wide number of registered domains on the internet recently, and daily more and more increase has been witnessed. These domains are used to carry out different scams, or they are used to act as a honeypot for the target users. Hackers get personal data through this procedure and then use it for their intended purposes. One of the main sources to lure the user into clicking on the link or downloading the malware are spam emails, for which the user becomes victim through mobile device or computers [6].

3.3 Malware and Ransomware

The covid-19 pandemic has accelerated the digital transformation in the world. From day to night, companies had to review their work models and offer their employees ways to enable remote work, thinking about the health and safety of their teams. This high number of professionals working from home and, at least at first, without adequate protection for companies access, networks, data, and intellectual property would naturally draw the attention of cybercriminals. Several surveys on digital threats have been published during this period and all point to an exponential growth of ransomware attacks, which are malware created and disseminated with the aim of blocking access to files or systems to release them after payment of a specified amount as if it were a virtual hijacking. The ransomware infects the system via email attachments, links, or through working employees whose credentials are already compromised by exploiting a vulnerability in their systems [6].

3.4 Spam emails

Another piece of true news during this time of pandemic was the amount of Phishing attacks that are usually detained two or three dozen people a year, but in the face of the pandemic. This social engineering attack, as we can see from the figures described above, has been highly used and efficiently.

Phishing is nothing more than a fraudulent attempt to acquire the other persons data by means of a disguise, which means trying to pass yourself off as a trustworthy person or entity, so that the person to be attacked has no problem in providing any kind of personal data due to their legitimate appearance.

This attack takes place mostly in the form of a message through e-mail forgeries or even through instant messaging if the hacker already has the persons phone number. As

a rule, this attack always has a reliable format as legitimate looking websites, offers not to be missed or even pretending to be a non-profit company to make the person feel in the scope of help.

Table 2. There have been numerous cases in which the intruders pretend to be from legit organizations such as WHO. They use domain spoofing to fool the victim that the email is coming from WHO and ask them to donate in bitcoins. For instance, the end of the email address normally ends with the organizations website, and people can know from there whether they are communicating with the right person or organization. The intruders use an email such as coronavirusfund@who.org. The WHO official website www.who.int ends with "int" and not with "org." Any user who did not confirm this email may become a victim [7].

3.5 Malicious Social Media Messaging

Nowadays, social media is very common and is almost in the reach of every individual. Hackers find it a great opportunity and tend towards the various social media platforms such as Facebook and WhatsApp. The attempts to obtain confidential information through fraudulent messages), spam (unsolicited email) and targeted attacks on social networking platforms. The scams typically lure victims into free subscriptions such as Netflix premium free account. When the victim clicks on the link, it redirects them to their social media phishing website. In some cases, it may ask to enter the credentials of their accounts.

From what has been described we can see that during the pandemic this was one of the most used attacks and with great efficiency, however, how to prevent such attacks. Unfortunately, we cannot simply install a software program or have the usual antivirus for prevention. Because we live in an age where there is great social exposure it is very easy for anyone or hacker to get their email, name, mobile phone. Because of this it is inevitable not to receive phishing emails.

The new pandemic landscape has shown that several companies have been forced to accelerate digital transformation processes. Digital transformation brings with its security considerations regardless of flexibility. Most users were working remotely as a result of the pandemic and it was also noted that the company, they were working for did not provide the necessary security tools to do the work remotely.

Although some companies had already adopted mechanisms to carry out the digital transformation process, many others ignored the three basic pillars for saying that a computer system is secure that it is: Confidentiality, Integrity and availability. But it is not the companies fault either because of the comfort of the home, some people ignored some care that we would have in the workplace. As a result, some workers pay less attention to cyber-security issues.

One of the big reasons for this is because employees use their own home equipment as a working tool. Working from home made it sound like a nice idea to many people, but it might bring some problems for companies because of Security. People have ended up neglecting security measures, which leads to compromising sensitive company data. From another point of view, it is reported that because there is more pressure on telework, employees ignore the recommended security measures.

4 Possible attack prevention

Companies and organizations need to prepare for the risks of cyber security. In recent months the threat called "sars-cov2" has made the area of security difficult due to the need to spread as much information about the virus as possible which has caused phishing emails to grow.

In this area it is necessary to understand the main risks that need to be faced and measures that we can take to ensure the privacy of companies and hacker personnel trying to take advantage of the vulnerabilities in this sector.

With the implementation of containment there was the idea of teleworking as mentioned above in this paper, companies enabled employees to take equipment that was in a business environment home. This led to a great danger of integrity due to the fact that most homes did not have a secure network. A recommendation in this environment will be to protect this equipment with data encryption, strong passwords so that it cannot be accessed by third parties and good practices of use such as blocking / logging out.

Another important measure will be the investment of a separate camera from the device and of good quality. With the containment the participation of teleconferences and video calls became important. However, it is need to be aware of the attacks that can be made these days. It is easy for a hacker or even an ordinary person to "hack" a camera and in order to be able to prevent this kind of attacks we should cover the camera whenever we are not using it and if the camera is separated from the device simply disconnect it.

Another procedure to keep in mind is the use of a VPN if employees need to access the companys internal network. It is recommended to do it inside the company or that the IT team creates a VPN so that employees at home can access the necessary resources in a secure way. This measure is quite clever as it ensures the privacy of any remote worker including this method ensures strong authentication and high encryption methods.

A good practice and investment will be in protecting the home network that ensures enhanced protection when working at home. Some methods to increase the security of the home network would be:

1. Create a unique strong password.
2. Changing the SSID name.
3. Limit MAC address access
4. Update the firmware

Companies should implement training to inform company employees of the dangers of cybersecurity is to conduct awareness campaigns to help combat cybercriminals who often try to exploit vulnerabilities.

In order to avoid this kind of attacks we must be careful with e-mails to which we are asked for personal data, usually reputable companies and banks do not make this information requirements of personal data.

We should try to avoid opening embedded attachments or links, as they may be loaded with malware. Usually, this kind of attacks may have unmissable offers and

grammatical errors and when we receive e-mails of this kind, we should be cautious and check if we are dealing with a legitimate company and if the link redirects us to a real link, one way to understand if we are in the presence of a real link is to pass the cursor on that same link and see the information in the bottom left corner that will show the real link. Unfortunately, in the face of the pandemic the great volume of attacks was not only phishing.

With the changes caused by the pandemic, hackers have adjusted new strategies so that they can profit from radical changes in the lives of people and companies.

5 Conclusion

In conclusion, we can see that the scenario is not at all favorable, either from a health point of view or from a safety perspective. If we think about the future in a positive way, people and companies may now pay more attention to safety and the risks behind it. That said, users are now more aware and aware of security risks and companies will be better prepared for when it is necessary to go back to remote work. With the recent outbreak of the coronavirus pandemic, there have been

A huge increase in the number of users interacting with each others working online. Taking advantage of the situation, the hackers IT is increasing daily, with the same ratio, there is an increasing cyber-security threats and privacy issues as well. There has been a considerable increase in the record of malicious attacks, websites, and spam e-mails. Intruders are targeting individuals, government officials and even doctors and health care workers care systems. This paper presented what happened during the pandemic and how people and businesses adapted to the new lifestyle derived from Covid-19 as well as the most commonly used hacking links. These cyber-security threats have led to some serious questions and concerns about personal data and the future of telework.

6 References

1. The official annual cybercrime report 2020. Herjavic Group. 2020. URL: https://tinyurl.com/y56trmgv
2. Naidoo R. Um modelo de influência de vários níveis do cibercrime com o tema COVID-19. Eur J Inf Syst 2020: 306-321. [CrossRef]
3. The WHO reports a five-fold increase in cyber attacks, calling for vigilance. World Health Organization. 2020 April 23. URL: https:. / / Www who.int/ fourth news / detail / 23-04-2020-which-reports-quintuple-in-ciber-attacks-impulses-surveillance

4. N. A. Khan, S. N. Brohi, and Jhanjhi. NZ, "UAV's Applications Architecture Security issues and Attack Scenarios: A Survey," in 1st International Conference on Technology Innovation and Data Sciences (ICTIDS) 2019, 2019
5. https://www.researchgate.net/publication/341324576_Ten_Deadly_Cyber_Security_Threats_Amid_COVID-19_Pandemic
6. S. Stein and J. Jacobs, "Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak," 2020. [Online]. Available: https://www.bloomberg.com/news/articles/2020-03-16/u-s-healthagency-suffers-cyber-attack-during-covid-19-response
7. Interpol," Covid-19 cyberthreats, "2020.: https://www.interpol.int/en/Crimes/Cybercrime/COVID-19- cyberthreats.
8. 25-WHO, "Beware of criminals pretending to be WHO," 2020. [Online]. Available: https://www.who.int/about/communications/cybersecurity.

Data Security and Privacy in Times of Pandemic

Luis Fernandes

Lusófona University, Porto - Portugal
a21805177@mso365.ulp.pt

Abstract. Our present is marked with the corona virus appearance, which lead to a worldwide pandemic situation declared by the world health organization. This situation leads to several different measures to prevent the virus from spreading, which includes online classes from schools and universities, homeworking in various organizations among a lot more of other measures. The data security and privacy are a matter that always concerns organizations and all the general public who uses internet. In these days that matter worries double or triple because most of this organizations were not prepared for this situation and most of them had to rush and made changes on their network to keep working and keep making money. For hackers this is a great opportunity to strike, make damage and profit from that. This paper will present several risks that the pandemic brought along in terms of cybersecurity. This paper will also show some possible preventions to these risks and responsibilities from several organizations that provides important services, that will keep our privacy and the data safe from intruders. This paper will also see some examples that happened during these times and what learn from those examples.

Keywords: Pandemic, Cybersecurity, Riscks, Preventions, Data security, Privacy.

1 Introduction

The coronavirus impact on the world was so big that the world health organization had no other options then declaring pandemic situation. This happen on 11th March 2020 [1] and forced governements and organizations to take measures, that include closing countrys, citys and curfew measures. Organizations and the population had to adapt to this measures wich revealed some vulnerabilities and opportunities for hackers to strike. Since the appearence of internet and it's integration on our lifes,work and in pretty must everything, the data security and privacy has been a consourne. This consournes increased because organizations were not prepared to make this changes, and were forced to maked them quickly in addiction this virus is new and the information about it was not transperant and a lot of wrong information was circulanting on the internet. Data security means protecting our digital data, from those who, without access, get our information, stored on the digital world, commonly known as hackers. This is a responsibility from the companies where we store our data, but it's more our responsibility then them, because most of the times we are the ones who give access to

10.11228/dpsc.03.01.003

that people without realising it. This happens because people don't take serious this matter and facilitate, thinking that the problems envolving this subject only happens to others. When we talk about data security problems, we talk about cyber attacks and data breachs. Data security is linked with privacy, because if we don't take data security serious and we see our information leaked this affects our privacy. On this report, will be analyzed the trend of cyberthreats during the covid-19 pandemic, defining the most common threats, showing some examples about them and how to prevent it. Further on this report will be explored the teleworking subject, the concerns and measures to improve cybersecurity.

2 Most common cyberthreats during covid-19 pandemic

A cyber attack is an attempt to change or disturb the three principles of cyber security, confidenciality, integrity, availability. Confidenciality means restricting access and share of the information on the system. Integrity means protecting the information from being changed or destroyed. Availability is keeping the system available for those who have access to it and unavailable for those who don't have access or not logged into the system. Inevitably, the pandemic lead to an raise on the use of computers and internet, this was a gold opportunity for hackers. This is a challenge for engineers who are responsible to keep systems safe, increasing data security, and people, by protecting their privacy.

2.1 Trend of cyberthreats

On the previous years, this cyber security challenges were already tough for engineers, because tecnology keeps changing, hackers keep evolving and it keeps being an exhaustive task with hackers only needing to find one vulnerability and engineers need to try find all vulnerabilities and keeping it from becoming a threat. Currently the challengs are even harder due to this virus and the necessaries measures that lead to an increase and change to the trend on the cyber attacks. According to the FBI Internet Crime Complaint Center (IC3) cyber attacks have increased with the pandemic [2]. The best way to protect from cyber attacks is to work from the organizations with strong security policies, but the best way to protect from the virus is to stay home where the security policies are weaker [3]. This balance is hard to manage and makes a big vulnerability for the organizations who saw their systems very vulnerables for hackers to strike.

Top cyberthreats 2019-2020	Trend
1. Malware	---
2. Web-based attacks	
3. Phishing	
4. Web application attacks	
5. Spam	

Table 1. Top cyberthreats 2019-2020 [4]

Following this report the covid-19 pandemic had direct impact on the changes from the previous years [5]. As mentioned this crisis lead to several changes, this changes alone are already significant and have a big impact on making systems vulnerabels to strangers. But this changes came with other problem, time, systems had to be adapt quickly because the covid-19 doesn't wait and every day more and more cases were detected. Making this changes quickly are risky because the probability of bringing other vulnerabilities to the table are big, also mistakes could happen and the impact won't be only on the system, this could implate all the organization. Phishing was one of attacks that went up on the ranking from the previous years [5]. The miss information and the fast appearance of the virus made an opportunity for hackers to profit from this social engineering attack. Hackers impersonated hospitals and other entities/business using possible fake cures to the virus [6], for example. Even the world health organization was impersonated by hackers on the hunt for information. These hackers have multiple intentions but the major one revealed on the report was for financial matters [4].

2.2 Definition and examples of the most common cyberthreats

To prevent a cyber attack is important to know all the different attacks, knowing how they work is the first step to prevent them from happening and affecting our systems.

2.2.1 Malware

Malware is the most common cyberthreats out there it comes in form of malicious software. On malware we include cryptominers, viruses, ransomware, worms and spyware. Hackers have a lot of intentions on attacking a system but the most common objetives are information or identity theft, espionage and service disruption [4]. The main inicial point for this attacks are steal the e-mail protocols, but due to covid-19 was noticed an increase of malware embedded in interactive coronavirus maps and websites[7]. In the malware family the ransomware was one of them that increased with the pandemic. Ransomware is an attack that target multiple directories encrypting the information on those directories. The encryption methods are very complex taking

years to unencrypt the information. Usually hackers send an email to their victims asking for money in exchange for the password to unencrypt the directory. The problem with this malware type is that hackers keep asking for money threatening to encrypt data again. The coronavirus made more preassure on hospitals, health centers, education and public institutions. Hackers toke this opportunity and lunched ransomware attacks to this organizations since they can't afford to be locked out of their systems. Hackers thought that these organizations would pay due to this reasons [7]. According to ENISA malware report [4] 71% of organizations experienced malware activity that spread from one employee to another, 46,5% of all malware in e-mail messages found in '.docx' file types, 50% increased in malware design to steal personal data and 67% of malware were delivered via encrypted HTTPS connections. The following chart shows the numbers of successful attacks using URLs that include the terms "COVID" or "coronavirus".

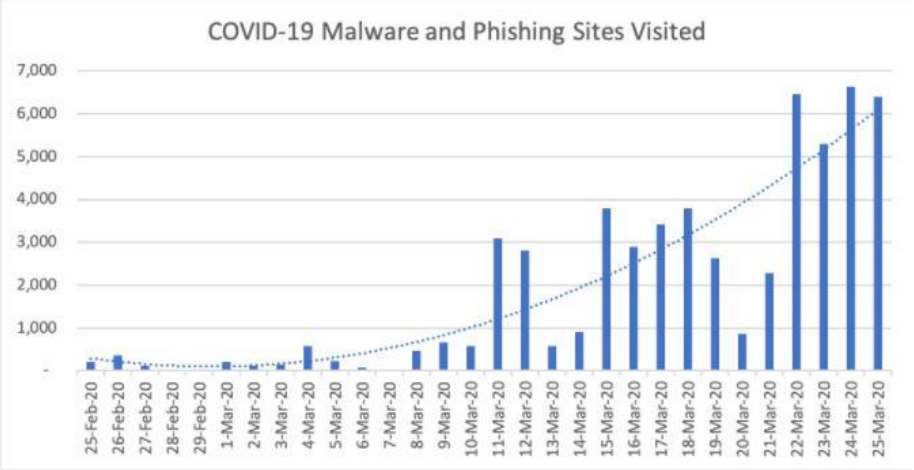


Fig. 1. COVID-19 Malware and Phishing Sites Visited [8]

Analysing the chart there is an exponential increase on the numbers on March 11, that was the day that World Health Organization declared the outbreak pandemic [1]. After that day, and has the trending line confirms, the number of successful attacks increased as the world population were searching for informations related to the pandemic.

2.2.2 Web-based attacks

On the past few years, the usage of web services have been increasing, due to the various advantages, including the no need to install software to have the same functions. The increased usage of this type of systems lead hackers to explore, find more and sophisticated ways to explore vulnerabilities on this systems. Web-based attacks are an attractive method since the increased usage of this kind of systems. There are multiple

attacks envolving this systems, for example malicious URLs or malicious scripts that directs the victim to a malicious website or even to download malicious content. Another common attack is to inject malicious code into a legitimate but compromised website to steal information, and other data. Other concern with these systems are the web browsers, although the browser are continuous updating and improving security measures, hackers always manage to find vulnerabilities. Different than previous years, the brute force attack increased on login systems in order to get on other users accounts. This kinda of attack affect the availability of web sites, APIs and could compromising confidentiality and data integrity. The most common attacks that happened on this systems are formjacking to steal user data, browser extentions and using online converters to download malicous software.

Description of the differents kind of attacks [4]:

- Formjacking - is an attack that injects code into legitimate websites. This attacks happen mostly on payment forms whos objective is to capture banking and other personal informations from the victims. When a victim is introducing their information on this infected forms, the injected code will also send this information to the attacker. The problem is that the original website works as intended, making it hard to know if this attack happened. With the pandemic the online shopping increased, making this type of attack a common one, taking advantage of the pandemic situation on the world.
- Browser extensions – There are several extensions, a lot of them are used because they help the users with functions that are not native on the browser. Anyone can make extensions, inclusive hackers making them with second intentions with the porpose of steal personal data and another types of attacks.
- Online converters – this is a common tool used by a lot of users, in most cases this tools ask the users to download the final data, converted. They use this to trick users and make them download malware to their computer. Hackers use this method to download various types of malware, but in the most cases ransomware is the most used type of malware [4].

During this pandemic another new cyber-attack was found, hackers used victims router more specifically the Domain Name Server(DNS) settings on D-Link or Linksys routers [7]. This attack opens the victims browser automatically, showing a notification from an malicious app. This notification tricked the victims to download an app called “COVID-19 Inform app”, this malware intended to steal browser cookies, stored passwords, browser history, transaction information and other data.

2.2.3 Phishing

Social engineering attacks on the past few years have been growing, becoming one of the most used attacks in the world. This kinda of attacks different than the others, it attacks the systems through the people instead of finding vulnerabilities and exploiting them or through very sophisticated and technical attacks. Phishing is the most common

attack on the social engineering family attacks. This attack is a fraudulent attempt to steal user data such as login credentials, credit card informations and other types of personal data. The majority of this attacks happens through e-mails, impersonating other entities or even the institutional e-mail of the organization. The objective with this e-mails is to persuade users to open malicious attachment or click on malicious URLs. For these tecniques make success hackers need to make a previous search to make appear the messages more authentic. This attack is based on emotional responses from victims. Even though most of the attacks use e-mails to connect with the victims the trend has been changing, appearing more and more cases using social media messaging for example via whatsapp. The methods are also changing and becoming more sophisticated, for example with the adoption of adversarial Artificial Intelligence algoritms to prepare and send messages. This attacks leads most of the time to unintentional insider threats. According to ENISA phising 2020 report, 26.2 billion of losses in 2019 with business e-mail compromise attacks, 42.8% of all malicious attachments were microsoft office documents, 667% increased in phishing scams in only 1 month during covid-19 pandemic and 32.5% of all the e-mails used the keyword 'payment' in the e-mail subject[4].

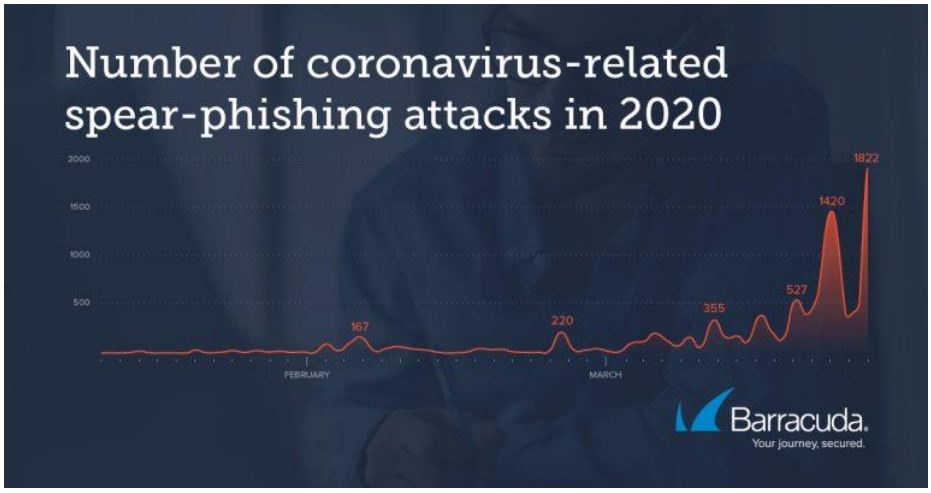


Fig. 2. Number of coronavirus-related-spear-phishing attacks in 2020 [9]

10.11228/dpsc.03.01.003

Fig. 3. Example of phishing scam related to the covid-19 pandemic [9]

This example is one of the many e-mails that were sent to inumerous of people trying to delude people to make donations that are allegedly to help an found rasing program.

2.2.4 Web application attacks

This attacks are similar to the one explained above. Web application and technologies become a part of our reality by adopting different uses and funcionalities. This applications through the years are becoming more complex, consequently growing the challenges to keep this applications safe and protecting the tree principles of cybersecurity. The common motivations with this attacks are financial or reputation damage and theft of critical or personal information. This services depend mostly on databases to store information. There are two big types of attacks on this systems, SQL (responsible for data bases) injection and Cross-site scripting (XSS) [4].

- SQL injection – This is a type of an injection attack, making it possible to execute SQL statements. These statements control a database server and this vulnerabilities bypass the application security measures. Hackers most commonly uses forms to input SQL statements, and possibly returning a complete database, compromising the confidenciality and integrity of the information [10].
- Cross-site scripting (XSS) – This is a client-side code injection attack. The hackers aim is to execute mailicious code on the victims browser, including the malicious

code in a legitimate web application. The common objective of this code injection is to steal the victims cookies, that has stored sessions, that can be used to get on the victims accounts [11].

According to ENISA Web applications report 20% of companies and organizations reported DDoS attack on their application services on a daily basis, 52% increase in the number of web application attacks in 2019 compared with 2018 and 84% of observed vulnerabilities in web applications were security misconfigurations [4]. With the pandemic hackers used the applications made to inform and give statistics to attack and profit from this world situation.

2.2.5 Spam

Spam consists of sending unsolicited messages in bulk. This is considered a cyber attack threat when used as an attack vector to distribute or enable other threats. Receiving spam is inconvenience, but it may also create an opportunity for a hacker to steal personal information or install malware. The most used way to send this messages is through e-mails. The difference between phishing and spam is that phishing is a social engineering technique that aims to steal user information and spam is just sending unsolicited e-mails to a bulk list. Phishing campains most of the times use spam techniques to distribute the messages. According to ENISA Spam report 85% of all e-mails exchanged in April 2019 were spam, 13% of data breaches were caused by malicious spam and 83% of companies were unprotected against e-mail-based brand impersonation. The covid-19 opened new doors, in middle February 2020 only a few hundred covid-19 attacks per day were reported, but on March 2020 more than 2500 attacks were happening per day [4]. One organization that was very inpersonated by hackers was the WHO (world health organization), the attackers used an e-mail such as coronavirusfund@who.org. The official website of the WHO is www.who.int , it ends with an .int different than the .org used by hackers.

2.3 How to prevent this cyberthreats

Every case is a case and for that reason there are different measures to prevent this cyberttacks from happening. But there are some common measures to prevent this attacks, this measures should be adopted on organizations and also on a personal level to secure and protect the information. One vulnerability that every organization has in common are the people, the system could be well protected but the people is always a concern because if one person is not responsible, hackers could exploit that and bypass security levels, even if the system is well protected. To prevent this from happing organizations and governements should countinue with formation lectures and campains to teach and show what this attacks can do and what precautions should they take. A most common problem is that people don’t take this matter serious and keep doing the same mistakes, until something bad happen.

2.3.1 Malware

- Implement malware detection for all inbound/outbound channels, including email, network, web and application systems in all applicable platforms.
- Inspect the SSL/TSL traffic allowing the firewall to decrypt what is being transmitted to and from websites, email communications, and mobile applications.
- Establish interfaces between malware detection functions and security incident management to establish efficient response capabilities.
- Use the tools available for malware analysis for sharing malware information and malware mitigation.
- Develop security policies that specify the process to be followed in the event of infection.
- Understand the capabilities of various security tools and develop new security solutions. Identify gaps and apply the defence-in-depth-principle.
- Employ mail filtering for malicious e-mails and remove executable attachments.
- Regulary monitor the results of antivirus tests, and keep those up do date.

2.3.2 Web based attacks

- Update internet browser and related plugins to keep them up to date and patched against known vulnerabilities.
- Make sure that endpoints and installed software are updated, patched and protected.
- Isolate applications and create a sandbox to reduce the risk of drive-by-compromise attacks.
- Websites owners, should hardening servers and services to mitigate web-based attacks. This includes controlling the version of the content scripts as well as scanning locally hosted files and scripts for the web server or service.
- Restricting web-based content is a technique to protect against this attacks. Facilitating tools such as ad blockers or javascript blockers will decrease the possibility to execute malicious code.
- Monitor web e-mail and filter content for detecting and preventing the delivery of malicious URLs and files/payloads.

2.3.3 Phishing

- Educate staff to identify fake and malicious e-mails and stay vigilant.
- Consider the use of a security e-mail gateway with regular maintenance of filters.
- Apply security solutions that use machine-learning techniques to identify phishing sites in real-time.
- Disable automatic execution of code, macros and preloading mailed links at the email clients and update them.
- Implement one of the standards for reducing spam e-mails, such as SPF, DMARC and DKIM.
- Use secure e-mail communication using digital signatures or encryption for critical information.

- Do not click random links, especially short links, checking always the domain name of the websites.
- Activate the two factor authentication to protect the accounts.

2.3.4 Web application attacks.

- Use input validation and isolation techniques for injection type attacks.
- Implement web application firewalls for preventive and defensive measures.
- Incorporate application security processes into the application development and maintenance life-cycle.
- Restrict access to inbound traffic for required services only.
- Deploy traffic and bandwidth management capabilities.
- Perfom vulnerability and risk assessments before and during the web application development.
- Conduct regular penetration testing during implementation and after deployment.

2.3.5 Spam

- Implement content filtering to locate unwanted attachments, mails with malicious content, spam and unwanted network traffic.
- Regular update the hardware, firmware, operating system and any driver or software.
- Avoid logging into new links received in e-mails or SMS messages.
- Use a secure e-mail gateway to regulate and automate maintenance of filters.
- Disable automatic code execution, macro enabling, preloading of graphics and mailed links.
- Regularly update whitelists, reputation filters and the real-time blackholeList.
- Use AI and machine learning for anomaly detection checks.

3 Teleworking and cybersecurity

There were inumerous measures taken by the governments across the world, according to the covid-19 numbers on their respective countries. But among all the measures there was one that almost every contry used, all the population needed to be in confinement. This lead to a major economy problem to pretty must every country if the population needed to stay home, how did the organizations work ? The organizations had no choice and as recommended by the WHO people had to start working from home, teleworking. The term teleworking before the pandemic was becoming popular but lot of organizations had issues implementing it. Most of organizations administrators have concerns letting their employees working from home, because it is hard to supervise and keep track on worked hours and satisfaction. Administrators had to put uncertainties aside and implement this measure. Another problem with the teleworking were the systems, if before the pandemic a lot of organizations were

already attacked, with teleworking the probability to be vulnerable was even higher. This implicates, private documents, messages, and other informations to be on the internet in order to communicate with other employees and with the applications. If it is hard to protect the information inside the organization with complex cybersecurity policies, engineers had a bigger problem in their hands to make this work without compromising cybersecurity. Information technology devices at home are generally perceived to be poorly configured compared to the work environment IT devices hence the IT devices at home are highly prone to cyber attacks especially due to these measures [12]. With employees on their homes, their network and their personal machines hackers can take advantage of the unsecured off-site routers, modems, unsecured network devices and poorly configured home network devices to exploit the vulnerabilities associated with teleworkers and compromising the security of the organization. That said its fair to say that organizations and people where not ready for these measures and because of that data security and privacy could become compromised.

3.1 Major security concerns with teleworking

As mentioned the teleworking presented IT engineers a lot of challenges, like those below, in order to protect the organization information [13]:

- Lack of physical control;
- Unsecured networks used for remote access;
- New threats for organizations through allowing external unsecured access to sensitive resources;
- Teleworkers may be using their own unstructured and unsecured resources to access their organizations valuable resources;
- The security measures assumes individuals uses computing devices from their employers wich is not applicable in all cases;

3.2 Measures to ensure data security and privacy with teleworking

To protect the organization from intruders and keep working using telework, the organization should take some measures like the ones below [13]:

- Developing and enforcing a telework security policy, such as having tiered levels of of remote access;
- Requiring multi-factor authentication for enterprise access;
- Using validated encryption technologies to protect communications and data stored on the client devices;
- Ensuring that remote access servers are secured effectively and kept fully patched;
- Securing all types of telework client devices, such as desktop and laptop computers, smartphones and tablets against threats;
- Train employees on cybersecurity in order to protect the organization;

4 Conclusion

Before the covid-19 pandemic data security and privacy were already a battle between hackers and engineers, the battle was not easy and the appearance of this virus was bad for the general world population health but also bad for the data security and privacy, with a lot of new attacks possibilities for hackers to explore. Helped wih the little time that engineers had do adapt the systems to the measures taken by governments and organizations, hackers profited a lot from this situation. Important now is to keep improving the security policies and hoping for this situation to end. It is also important, when this ends, to make more studies about the real problems that this situation brought and analyze what could be done better and learn from that and hopefully if something similar happens again we are prepared to face these kind of challenges.

References

1. Declaration of pandemic situation by WHO, https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020, last accessed 2020/11/06.
2. FBI public service announcement, https://www.ic3.gov/Media/Y2020/PSA200401, last accessed 2020/11/06.
3. André Barrinha.: Cibersegurança em Tempos de Pandemia. In CIBERSEGURANÇA E CIBERDEFESA EM TEMPOS DE PANDEMIA. IDN 2020.
4. ENISA Threat Landscape.: List of top 15 threats, From January 2019 to April 2020.
5. ENISA Threat Landscape Report 2018.: 15 Top Cyberthreats and Trends, January 2019.
6. Advisory: Covid-19 exploited by malicious cyber actors, https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory, last accessed 2020/11/11.
7. Navid Ali Khan, Noor Zaman and Sarfaz N. Brohi.: Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. ResearchGate (2020).
8. Sophisticated COVID-19–Based Phishing Attacks, https://www.menlosecurity.com/blog/sophisticated-covid-19-based-phishing-attacks-leverage-pdf-attachments-and-saas-to-bypass-defenses, last accessed 2020/11/25.
9. Threat Spotlight: Coronavirus-Related Phishing, https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/, last accessed in 2020/12/06.
10. What is SQL Injection (SQLi) and How to Prevent It, https://www.acunetix.com/websitesecurity/sql-injection/, last accessed in 2020/12/06.
11. Cross-site Scripting (XSS), https://www.acunetix.com/websitesecurity/cross-site-scripting/, last accessed in 2020/12/07
12. Arnold Mashud Abukari and Edem Kwedzo Bankas.: Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond. 4, April-2020
13. Karen Scarfone, Jeffrey Greene, and Murugiah Souppaya.2020. Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions. ITL BULLETIN MARCH 2020.
14. Alya Hannah Ahmad Kamal, Caryn Chuah Yi Yen, Mah Hui Ping and Fatima-tuz-Zahra. September 2020. Cybersecurity Issues and Challenges during Covid19 Pandemic.
15. Bernardi Pranggono and Abdullahi Arabo. 2020. COVID-19 pandemic cybersecurity issues.

Social Engineering Attacks: Risks, Vulnerabilities and Countermeasures

Luís Costa

Lusófona University of Porto, Portugal
luiscosta205@gmail.com

Abstract. Social engineering is the procedure of fooling someone to act or give information. The attacker tries to take advantage of the victim preferences, needs or emotional state.

In the past some people practiced social engineering, going door-to-door, trying to lure people to give them money or information in exchange for products/services that they supposedly needed. In some, if not most cases, it was a scam. Nowadays this technique evolved and its mostly used online.

This study will show the tactics used by the attackers and how they execute, the risks involved, how to prevent getting caught in one of these situations and if some type of intervention can reduce the effects. By the end of the paper, it's expected to understand how social engineering is executed and some ways to prevent it with security policies and security training awareness, for example.

In our fast-evolving reality, the population needs to get/maintain informed and updated about this problem and learn how to evade it.

Keywords: Social engineering, Persuasion, Prevention, Risks, Awareness, Vulnerabilities, Countermeasures, Security, Phishing

1 INTRODUCTION

The technological world is evolving at a significant pace with the growth and availability of technologies making this one of the main reasons for the fastest and powerful growing of brands, markets and companies [1]. These companies work with online transactions, social networks and have loads of data and information stored on the internet. This stored information looks appetizing for the cyber-criminals and while technology evolves, the number of cyber-criminal attacks and their complexity evolve as well, causing cyber security to play an important role [2].

To prove and demonstrate the cyber-attacks evolution and money involved, on the 2018 Internet Crime Report, the Federal Bureau of Investigation (FBI) received a total of 351.937 complaints with an estimated loss of $2.7 billion [3] and, just a year later on the 2019 Internet Crime Report, received a total of 467.361 complaints, an average of nearly 1,300 every day, with an estimated loss of $3.5 billion [4], showing an increase of at least 100.000 complaints and an estimated loss increase of $800 million in just one year. The data mentioned above are only related to the United States of

10.11228/dpsc.03.01.004

America. According to Cybersecurity Ventures, in 2021, it's expected a monetary loss of $6 trillion worldwide (more profitable market than all major illegal drugs combined), while, in 2015, the real cost was only $3 trillion. These numbers tend to increase annually due to the access to technologies and the internet all over the world [5].

The information systems safety doesn't solely depend on technological countermeasures, the human factors are a huge problem too when it comes to security. Social engineering attacks explore the human factors in order to obtain information and/or access to something. This type of attack succeeds because of human flaws, like the human's natural helpfulness, psychological weaknesses and the underestimating of value of the information they possess [6]. The human component is indispensable for the operations of every company and its also the most vulnerable component to attacks in a company [7].

This paper will focus on the social engineering type of attack. Section 2 will focus on the definition and origin of the concept "Social Engineering" and its subsections will approach types of social engineering attacks, vulnerabilities and countermeasures. At the end of this paper, on section 3, will be a demonstration on how to create a social engineering attack (email phishing attack) on the SET (Social Engineering Toolkit) that comes previously installed on Kali Linux.

2 SOCIAL ENGINEERING

The concept of "social engineering" on the cyberspace field has been around since, at least, 1995, when it was used in the article "Cracking a Social Engineer" by Al Berg, but it has been practiced on other fields (social and political) for much longer [7]. The term was found at the early 20th century on the political field related to social problems, but, at that time, it had a positive connotation. That positive connotation started to change since World War II, when politicians started using this technique to gain electoral advantage [8].

According to [9], social engineering is defined as "influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation" and its acknowledged as being one of the greatest threats to the security of businesses.

As stated in [10], social engineering is an act "to manipulate people, by deception, into giving out information, or performing an action".

In short, social engineering refers to humans as the weakest link because people can be manipulated and persuaded into providing information to attack computer systems or to perform actions that furnish network access to the attacker [11][12].

The attacks on the social engineering field can be classified into two groups (human based and computer based), as represented in Figure 1 [8][13]:

10.11228/dpsc.03.01.004

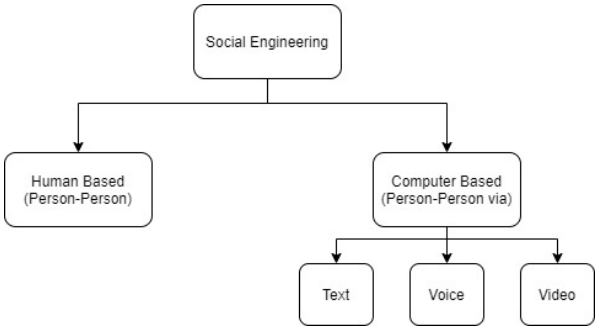


Fig. 1. Classification for social engineering attacks.

Human-based attacks consist in attacking in person (face-to-face) in order to obtain information. This can be achieved by impersonating a real or fake person.

Computer-based attacks are performed using devices. This type of attack can strike multiple victims in seconds. They can occur via text, voice or video.

It's possible to reconcile the two types of attack in one single attack [8][13].

2.1 Attack Phases

Social engineers use a set of techniques to gain the confidence of their victims. While there are several social engineering attack techniques, Kevin Mitnick [9] created a common methodology to all of these attacks, composed by 4 steps on how to establish a trust relationship with the victims, represented on Figure 2 [12][13][14]:

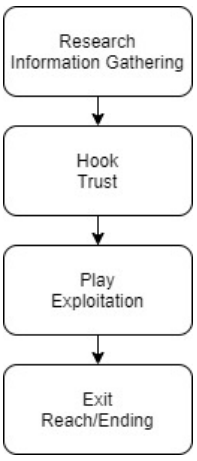


Fig. 2. Attack phases for social engineering attacks.

In the research stage, the attacker chooses the target and tries to gather all the information he cans to create a connection with the victim, while trying to establish some attack possibilities. Next comes the trust phase, also known as relationship development phase, where the attacker starts creating a relation with the victim. Is known that people tend to give away information when they trust someone. In the play/exploitation phase, is expected that the victim already trusts the attacker. The attacker then, tries to exploit the victim to provide private information or to do certain actions through manipulation. In the final step, exit phase, the attacker terminates the interaction with the victim, without raising suspicion preferably, and uses the gathered information to procced to the objectives of the attack [12][13][14].

2.2 Risks

Risk can be perceived as "the possibility that something unpleasant or unwelcome will happen", also known as an attack. For a risk to exist, it must have an associated impact and probability. Impact can be understood as damage, and probability is the chance of the risk happening. If there is no probability of happening, then it's not a risk [10].

2.2.1 Human Based Attacks.

2.2.1.1 Impersonation.

Impersonation consists on the attacker assuming a false or real identity (employee from a targeted company, for example) to keep his real personal identity safe while carrying out an attack to gather information or manipulate someone. It's easy to execute this type of attack and it requires little preparation. Usually is combined with other attacks like tailgating, piggybacking, pretexting and/or reverse social engineering [8][14].

2.2.1.2 Tailgating.

Tailgating is following an authorized person to gain access to restricted areas. It can be considered legal or illegal based on the circumstances. This attack is getting easier to execute because of public databases like LinkedIn, that reveal the organization positions and the name of the people who occupy these positions. [8]

2.2.1.3 Pretexting.

Pretexting can be simply explained as obtaining information under false pretense. For that is necessary a good, fake and convincing story to be able to collect the desired information. Normally is necessary to impersonate an important entity to carry out with this attack, and that requires a lot of preparation [8][13][14].

10.11228/dpsc.03.01.004

2.2.1.4 Reverse Social Engineering (also known as quid pro quo).

The attacker impersonates as a person with authority and manipulates the victim to ask the questions instead of the attacker. One approach, for example, used with this type of attack is to previously compromise the network of an organization and then appear with the solution to solve the problem he created, assisting the company in question and gaining trust from the employees. Then he asks the victim to log into the network, achieving his final goal [8].

2.2.1.5 Eavesdropping.

Eavesdropping is when sensitive information is being talked out loud, thinking that only authorized personnel are listening while the attacker is also listening. It can also occur through telephone lines and e-mails [14][15].

2.2.1.6 Dumpster Diving.

The attacker gathers information through the targeted organization's trash. Oftentimes, companies dispose the garbage with documents and even old hardware that contains sensitive information [13][14].

2.2.1.7 Shoulder Surfing.

Shoulder surfing consists on watching the victim writing sensitive information or authentication data [13][14].

2.2.1.8 Piggybacking.

Piggybacking is when an authorized person allows an unauthorized one to enter in a network or physical place (intentionally or unintentionally) [16].

2.2.2 Computer Based Attacks.

2.2.2.1 Phishing.

Phishing is the act of disguising as a trustworthy entity to acquire private information or authentication. This attack is mainly executed through e-mail [8]. Usually this type of scam creates a sense of urgency on the victim in order to manipulate them to act without judging the situation properly [17].

2.2.2.2 Pop-Up Windows Attack.

Pop-Up Windows attacks are windows that appear when visiting a website or when the machine is infected with a malware, that ask for login credentials under the excuse of loss of connection with the server, for example. This attack can also deceive the target under the premise that they won some sort of contest or prize, asking, then, for credentials and personal information or injecting malware on the device [13][16].

2.2.2.3 Baiting.

Baiting, as the name implies, consists in creating a bait, like leaving a USB drive or external disc containing a malware in a public place to be found by the target, that later on, will plug to the computer infecting all the network. Normally the malware

attacks on the background, so the victim doesn't know that it's being attacked [13][14][17].

2.2.2.4 Watering Hole.

This attack consists on knowing the legitimates websites that the victim visits often and afterwards search for vulnerabilities in it, infecting the website and waiting for the victim to fall into the trap [14].

2.3 Vulnerabilities

As mentioned before, humans are the weakest link on an organization. Companies could invest millions of dollars on technical security but still have their data compromised, because people need to get educated and informed about the risks and how to proceed on these types of situations [17].

According to [10], there are five flaws of the human psychology that make them vulnerable to social engineering attacks: Follow Instructions, Ignorance, Gullibility, Desire to be Liked and Being Helpful.

2.3.1 Follow Instructions.

Humans tend to think that they decide if they will follow instructions or not. But, in reality, lots of people are getting manipulated every day to do things without questioning. The military, for example, is trained from day one to follow instructions and orders without questioning their superiors. The same can happen when an employee thinks he's talking with some authority entity or superior.

2.3.2 Ignorance.

People, when feeling ignorant, are more open to follow instructions. The IT (Information Technology) field is vast and isn't known by most people and social engineers know that and take advantage of it. If the victim senses he's talking with an expert, they will believe everything and do what they say. This doesn't mean that only people considered less intelligent fall for social engineering attacks.

2.3.3 Gullibility.

When people are offered attractive benefits, their naivety increases. One famous example is the "Nigerian prince" scam. People would receive an e-mail from an alleged Nigerian prince saying that the receiver was a legitimate heir to his inheritance. It was a social engineering attack, where the attacker tried to steal money and information.

2.3.4 Desired to be Liked.

Everybody wants to be liked. In the past, some people connected romantically with foreign diplomats in order to obtain private information.

2.3.5 Being Helpful.

Individuals are encouraged to be helpful in a business environment. Social Engineers use masquerading techniques to impersonate new employees, asking questions about private information, with the excuse that they only need help.

2.4 Countermeasures

Before everything, it's necessary to understand that social engineering attacks can occur to any individual, from executives to cleaning employees. It's important, as well, to perceive that it is impossible to reduce social engineering attacks to zero. What can be done, in that aspect, is mitigating risks and possible damage to infrastructures and data [18].

A good solution to reduce the success of social engineering attacks in an organization, is a multi-layered/multi-level approach, composed of five levels: Foundational level, Parameter level, Fortress level, Persistence level and Offensive/Gotcha level [18][19].

2.4.1 Foundational level.

The roots of information security are the policies. A security policy defines the standards and the level of security of the network and provides procedures and guides for the data and system protection of an organization. It also makes the employees aware of the importance of information's value. Some of the policies that can be found in that document to prevent social engineering attacks are: access approval, password changes and the destruction of confidential documents and old hardware, for example [6][18][19][20].

2.4.2 Parameter level.

Parameter level is the second level and consists in training all users about security awareness. The security policy should be used as a training complement, providing guidelines and motivation. In this level, users will learn about information that can be used by social engineers and types of conversations that they use [19].

2.4.3 Fortress level.

The third level, fortress level, consists in the resistance training of the core staff. Core staff includes everybody that needs to help or talk with the public, for example customer service, help desk and receptionists. The objective of resistance training is to make harder to persuade the key employees, preventing information leaks. This level can be complemented with punishment for employees that break the security policy rules and reminders of the security policy itself [18][19].

10.11228/dpsc.03.01.004

2.4.4 Persistence level.

At this level, all the users are reminded, through ongoing reminders, about the necessity of information security. The reminders must be creative and exposed regularly [18][19].

2.4.5 Offensive level/Gotcha level.

Finally, the last level occurs when an attack is happening. The victim will have procedures in place if he suspects that he is experiencing a social engineering attack. To do that, the employee can create traps, called Social Engineering Land Mines (SELMs), that will be able to expose and stop the attackers advance. There are a lot of traps that can be implemented, being the most-known call backs by policy, key questions to the suspect and centralized security logs [18][19].

3 Phishing Attack Example

As previously described, phishing is the act of masquerading as someone in order to scam victims for information or money. People are constantly being victims of phishing and one way to prove that is by visiting the spam folder of their personal e-mail, for example.

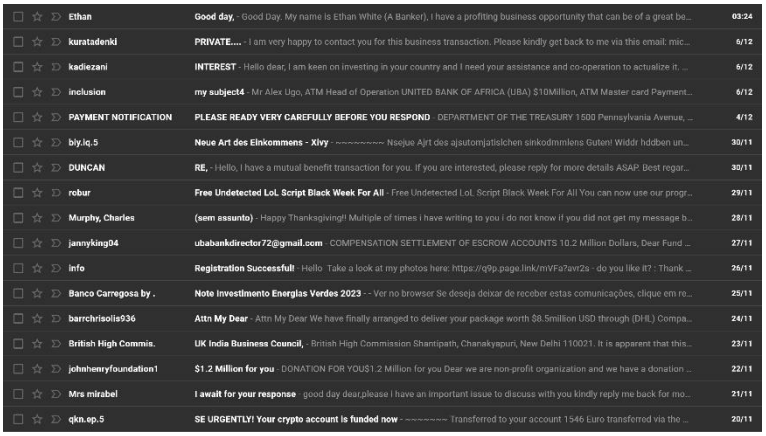


Fig. 3. Spam folder example.

As shown on figure 3, there are a lot of e-mails claiming that the addressee won money from some supposed bank or fake entity. A way to forge this type of attacks is through a toolkit called Social Engineer Toolkit (SET), that comes pre-installed on the Linux distribution Kali Linux.

Kali Linux is a Linux distribution based on the Debian GNU that helps companies auditing and penetration testing their IT security systems. This project started back in 2012 when Offensive Security (creator of Kali Linux) wanted to upgrade their last Linux project (BackTrack Linux) that could only be manually updated. This distribu-

tion was specifically created to help security professionals and IT administrators [21]. Social Engineering Toolkit is a product created by TrustedSec and was developed on the language Python. With SET is possible to test a large variety of social engineering attacks making it come in handy for every penetration tester and security professional [15].

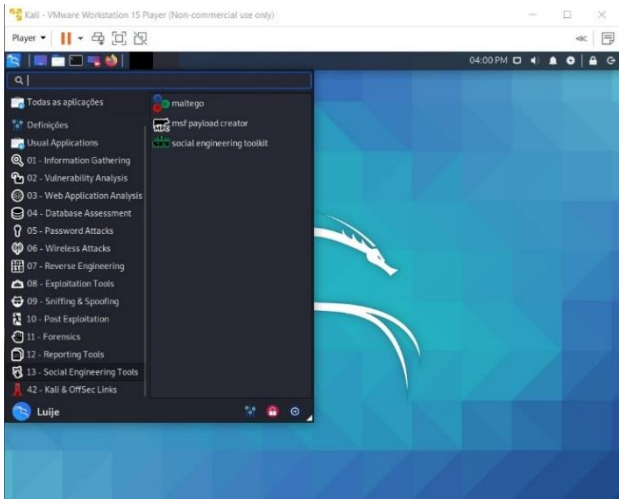


Fig. 4. Pre-installed social engineering tools on Kali Linux.

When opened, SET will provide a menu with seven options. Since this study will exemplify a phishing attack via e-mail, the first option was selected (Social-Engineering Attacks), that will open the attacks type list. From there we can choose the desired attack from the list as shown on figure 5.

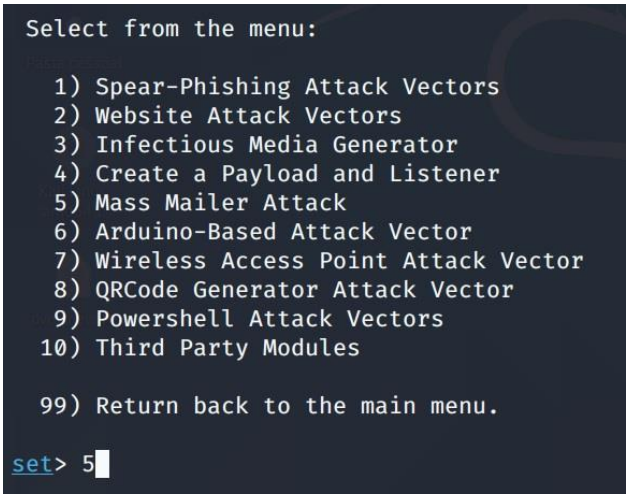


Fig. 5. List of SET attacks

Phishing attacks can be done in two ways on this toolkit: through Spear-Phishing Attack Vectors (focused on website phishing) and Mass Mailer Attack (focused on e-mail phishing). In this case, the Mass Mailer Attack was chosen because the demonstration is about e-mail phishing (Fig.5). After entering the Mass Mailer Attack menu, two options appear: "Attack Single Email Address" and "Attack Mass Mailer" (Fig.6). For the sake of simplicity and demonstration, "Attack Single Email Address" was selected since it only attacks one victim.

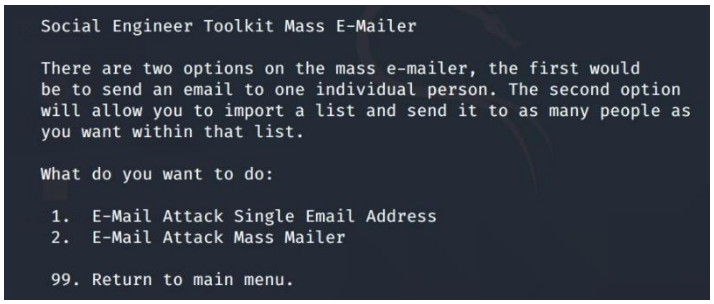


Fig. 6. Mass E-Mailer menu.

After that, some questions will be prompted, asking the receiver email and the sender email, password and "from name" (Fig.7). It will also be possible to flag the e-mail as high priority and to attach files (attackers can attach infected files/malwares). Then the attacker can write the subject and the body of the e-mail and send the attack (Fig.8).

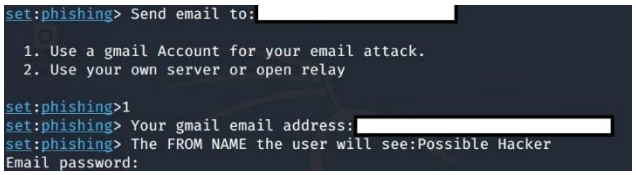


Fig. 7. E-mail related questions.

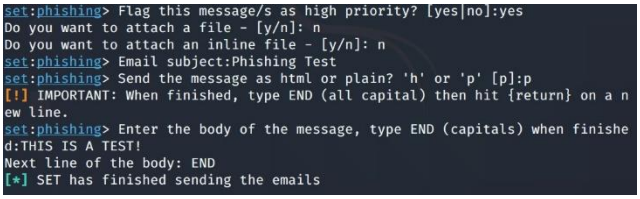


Fig. 8. E-mail content related questions.

Finally, the result will appear on the victim e-mail inbox or spam folder (Fig.9).

10.11228/dpsc.03.01.004

Fig. 9. Attack result.

This attack was executed only on one victim, but if the number of target e-mails is bigger, the chance of success increases immensely.

4 CONCLUSION

The expression "Knowledge is power, data is money" [22] couldn't be more relevant nowadays and on this matter, because that's what attackers try to do illegally, steal data for their benefit. The access to the world wide web facilitated that process, due to the availability of tutorials and software online that teaches and helps the attackers how to forge an attack, making it even easier to execute one. On that matter, social engineering is one of the most dangerous attacks currently, because it doesn't require a lot of computer knowledge to be successful which reinforces the idea that is necessary to teach and inform people about the dangers that this type of attacks can cause for companies and even personally and the best ways to prevent it from happening. In conclusion, studying social engineering should be one of the principal focus on the cyber security field, paying special attention to better and more efficient countermeasures, since it's evolving to be one of the most dominant attack vector in the future and organizations and people in general should be better prepared when that happens.

REFERENCES

1. Sood, A., Tellis, G.: Technological Evolution and Radical Innovation. Journal of Marketing. 69, 152-168 (2005).
2. Bendovschi, A.: Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance. 28, 24-31 (2015).
3. Federal Bureau of Investigation: 2018 Internet Crime Report. (2018).
4. Federal Bureau of Investigation: 2019 Internet Crime Report. (2019).
5. Cybersecurity Ventures: 2017 Cybercrime Report. (2017).
6. Luo, X., Brody, R., Seazzu, A., Burd, S.: Social Engineering. Information Resources Management Journal. 24, 1-8 (2011).

7. Y.Conteh, N., D.Royer, M.: The Rise in Cybercrime and the Dynamics of Exploiting the Human Vulnerability Factor. International Journal of Computer (IJC). 20, 1-12 (2016).
8. Ivaturi, K., Janczewski, L.: A Taxonomy for Social Engineering attacks. CONF-IRM 2011 Proceedings. 15, (2011).
9. Mitnick, K., Simon, W., Wozniak, S.: The art of deception. Wiley, Hoboken, N.J. (2013).
10. Mann, I.: Hacking the Human: Social Engineering Techniques and Security Countermeasures. Gower Publishing Limited, Hampshire, England (2008).
11. Laribee, L., Barnes, D., Rowe, N., Martell, C.: Analysis and Defensive Tools for Social-Engineering Attacks on Computer Systems. 2006 IEEE Information Assurance Workshop. (2006).
12. Gallegos-Segovia, P., Bravo-Torres, J., Larios-Rosillo, V., Vintimilla-Tapia, P., Yuquilima-Albarado, I., Jara-Saltos, J.: Social engineering as an attack vector for ransomware. 2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON). (2017).
13. Salahdine, F., Kaabouch, N.: Social Engineering Attacks: A Survey. Future Internet. 11, 89 (2019).
14. Breda, F., Barbosa, H., Morais, T.: SOCIAL ENGINEERING AND CYBER SECURITY. INTED2017 Proceedings. (2017).
15. Patel, R.: Kali Linux social engineering. Packt Pub., Birmingham (2013).
16. Maan, P., Sharna, M.: Social Engineering: A Partial Technical Attack. International Journal of Computer Sciences Issues. 9, (2012).
17. Conteh, N., Schmick, P.: Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research. 6, 31-38 (2016).
18. Ghafir, I., Prenosil, V., Alhejailan, A., Hammoudeh, M.: Social Engineering Attack Strategies and Defence Approaches. 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). (2016).
19. Gragg, D.: A Multi-Level Defense Against Social Engineering. Sans Institute 2003. (2002).
20. Saleem, J., Hammoudeh, M.: Defense Methods Against Social Engineering Attacks. Computer and Network Security Essentials. 603-618 (2017).
21. Hertzog, R., O'Gorman, J., Aharoni, M.: Kali Linux revealed. Offsec Press, Cornelius, USA (2017).
22. Rossi, B.: Knowledge is power, data is money - Information Age, https://www.information-age.com/knowledge-power-data-money-123458725 (Accessed: December 05 2020).

Social Engineering Attacks: Risks, vulnerabilities and Countermeasures

Nelson Cacheira[1]

[1] ULP – Lusófona University, Porto - Portugal

nelson_cacheira@hotmail.com

Abstract. Never before was the Internet the ground for communications and social interactions. The world is now a digital expansion of our lives, and the way we think and communicate. As digital interactions take ever more space in our personal life, the information given by the users to these platforms are in great jeopardy due to the inherent vulnerability of attacks. It is not uncommon to hear about attacks happening in companies, but it is something that is not taken into account by the common user, because it doesn't affect them. But if cybersecurity isn't taken into consideration, the next attack could be directed at us. Social Engineering should not be avoided or downplayed, and the discussion must be brought to the public eye, and discuss the risks, vulnerabilities, attacks and countermeasures. Attackers can easily take advantage of these vulnerabilities and exploit them for personal gains. Norms have been taking place such as cookie and privacy policies so the websites and corporations are clearer in their practice. The public must be aware of the risk they're facing, and put into practice ways to be safe online. This paper will explain the risks, vulnerabilities and ways to prevent these attacks.

Keywords: Social-Engineering, Cyber-Security, Internet Safety, Awareness, Countermeasures.

1 Introduction

Cyber security has become a new concern in the 2000s. Companies and private individuals are concerned with the leaking of information. The communications channels have widened, even at the workplace, being more popular the BYOD (bring your own device), in which these mobile devices carry around corporate information and have no way to be totally in the control of the companies [1]. Social media is too a great concern, being generally used by all ages and cultures. A study on "User characteristics that influence judgment of social engineering attacks in social networks" show for example, that perceived risk and perceived severity of threats vary between genders, being the women more aware than men [2]. Social engineering isn't only an online

problem. Even before the advent of the Internet, there were social engineering attacks going on. Now it just took to another level. The focus of this study will be on defining Social-Engineering, it's Categories, the hacker's motivations for attacks, the attack phases, types and vectors, to highlight the prevention and some methods anyone can apply to mitigate the problem. The objective is to bring awareness to the problem, and give some insight into what is Social-Engineering.

2 Social-Engineering

"Social engineering is the art of getting users to compromise information systems. Instead of technical attacks on systems, social engineers target humans with access to information, manipulating them into divulging confidential information or even into carrying out their malicious attacks through influence and persuasion" [3]. The Human factor is maybe the greatest threat to cybersecurity. If a software has programming errors, it is attributed to the Human not programming it correctly, and if there is a breach in security, it is because humans didn't take it into account when designing its defenses. Most of the issues come from people downplaying the importance of knowledge and awareness, trusting the website or application their using, and believing they're good at detecting such attacks [3]. In this chapter will be explained the categories, motivations, phases and types of social-engineering attacks.

2.1 Categories

Hunting. "This approach seeks to execute the social engineering attack through minimal interaction with the target. Once the specified objective is achieved and the security breach is established, communication is likely to be terminated. This is the most frequently used methodology to support cyber-attacks and as a rule, the modus operandi involves a single encounter" [4].

Farming. "Social engineering farming is not often practiced, nevertheless this technique may be used for situational purposes. The attacker aims to establish a relationship with the victim in order to extract information for a longer period of time. Throughout the process, the interaction can change, the target may learn the truth and the social engineer may attempt to bribe or blackmail the target, thus resorting to traditional criminal behavior" [4].

2.2 Hacker's motivation

For any crime, there is a motive worthy of pursuing. Being it the thrill of the moment, or financial games, there are various motives for attacks to take into consideration [5].

10.11228/dpsc.03.01.005

Self-Education. Can be only for the thrill of gaining knowledge and beating the system [5].

Financial Gain. Maybe the most thought of motive, blackmail and organized crime [5].

Revenge. Some ex-employees can exploit their known weaknesses of the system to get back at the corporate entity or an individual in the organization [5].

External Pressure. The social engineer can manipulate someone to break security protocols, by blackmailing, ransoming, exploiting moral dilemmas or extremist beliefs. Since there are no victims, just ones and zeros, the victim can be persuaded to commit a crime they wouldn't have in normal conditions [5].

Terrorist and Political Motivated Groups. Attacker can act on religious beliefs or activist values to break havoc and attack a financial and critical information infrastructure [5].

2.3 Social-Engineering Attack Phases

"Any criminal act has a common pattern. Such a pattern is evident with social engineering, and it is both recognizable and preventable." [6] When planning an attack, the social engineer plans his actions ahead. While the target doesn't know, the attacker can have already planned out who the target is, and how to get the information. Attacks of this nature, typically consist of four distinct phases: research, hook, play and exit, as shown in **Fig. 1** [4].

Research. This involves gathering information on the target. A variety of techniques can be used to achieve this, and be used to create a relationship [5]. An experienced social engineer can exploit chance encounters too [4].

Hook. This is when the attacker builds a relationship with the target. This relationship will be exploited an explored to capitalize on the created trust. Sometimes masquerading as a senior member of the organization or as a friend [5].

Play. Here is where the attack takes place, using the information gathered, the attacker performs the attack per se, to disclose or compromise the system [4][5].

Exit. The social engineer has completed his task, preferably without arising suspicion, because these attacks aren't easy to track down [4].

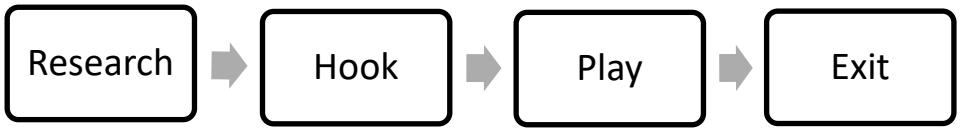


Fig. 1. Social Engineering Phases (4).

2.4 Types of Social-Engineering Attacks

Social Engineering attacks can come from two Operators. One being the Human, and the other Software [3]. Since the dawn of humanity, social engineering tricks have been occurring, especially with street performers and con-artists, but in the digital era, these tricks have taken another form, sometimes more indirect, through channels like e-mail, instant messaging, telephone, social networks, cloud services and websites [3]. **Fig. 2** shows the various ramifications of this, branching from Type, Operator and Channel.

2.4.1 Physical

These are physical interactions, such as eavesdropping, over-the-shoulder and dumpster diving. Can sometimes be the most practical and available method since no IT knowledge is needed to intercept conversations, check on passwords or steal an authentication card [3].

2.4.2 Social. This is the basis for all Social Engineering attacks. From even before the digital era, con-artists would use tricks to persuade into his biddings. These persuasion techniques are used to manipulate and address the curiosity of the victim, even to the point of developing and maintaining a relationship with their future victims, being the most prevalent attacks performed by phone [7]. Can lead to attacks such as baiting and spear-phishing attacks [3].

2.4.3 Socio-Technical. This is an approach that relies on technical knowledge for social engineering attacks. The best example would be the attacks via e-mail or instant messaging. These classic attacks like phishing are not lucrative, being aimed at a large number of people indiscriminately [8]. That is why these Socio-Technical attacks evolved to Spear-Phishing or Wailing, that target specific individuals [3].

2.4.4 Technical. Tools are used to gather and harvest information on future victims through malware or search engines to gather personal information about future victims [3].

2.4.5 Reverse Social-Engineering. There's still this often-overlooked type of attack. In this reverse take on social engineering, the attacker makes the victim think they're a trustworthy entity instead of making the first contact. That could be done by advertising and then assisting previously sabotaged victims [9]. Doors can be opened, and passwords can be given to the attacker directly from the victim, with the objective to help her [3].

10.11228/dpsc.03.01.005

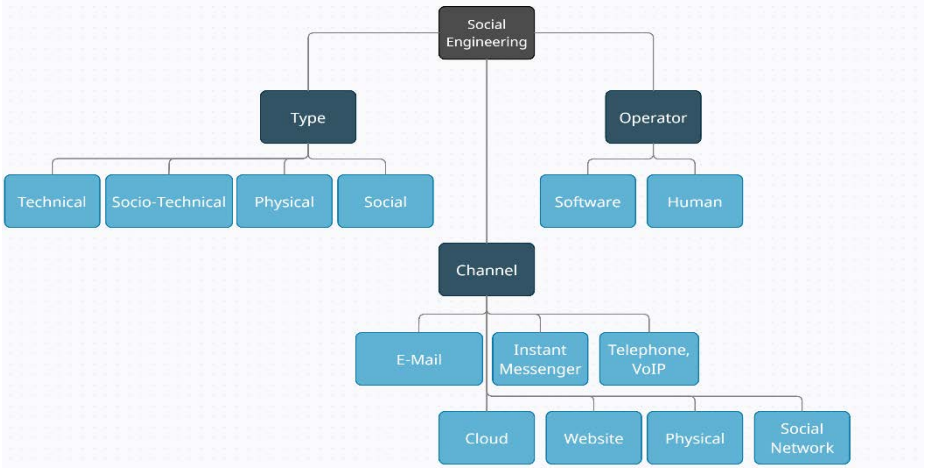


Fig. 2. Social Engineering Taxonomy [3].

3 Attack Vectors

Attacks can take on many forms. From waiting for any unaware victim as a trap, disguised as another person or website, or from directed spear-headed attacks on multi-millionaire corporations for financial or political gains, the creativity and genius of these attacks are ever evolving, always finding new ways to swindle the victims or breaching into high-security websites, as shown in **Fig. 3**. It does come to show the attackers will always be one step ahead.

3.1 Phishing

The act of illegally accessing to the information of the target, often masquerading as a trustworthy entity. Usually targets a large group of victims indiscriminately through various mediums [3].

3.2 Spear-Phishing

Is a targeted Phishing attack, used to hit specific individuals or companies after gathering the victim's information. Usually is meant to hit high-profile victims, with the intent to access the victim's system, to gather for example, company/military/personal secrets. It is highly effective, due to the preparation and focus involved [10].

3.3 Spy-Phishing

Is the act of spying on a victim through unauthorized installed software. The attacker installs a malicious software called spyware, by exploiting website fragilities, trojans,

or via Freeware and Shareware. waits the victim to access a predetermined website to steal log in information [10].

3.4 Dumpster-Diving

Is the act of going through the victim's trash. Has a man's trash can be another man's treasure, often the victims don't realize the problem imposed by their trash. The attacker can find login passwords, security footage, signatures, memos, personal contacts or e-mails [3].

3.5 Shoulder Surfing

The simplest method of gathering info, the eavesdropping. It is the easiest way to gather information, just looking at someone's phone or computer screen [3].

3.6 Advanced Persistent Threat

Refers to long-term, mostly Internet-based espionage attacks conducted by an attacker who has the capabilities and intent to comprise a system persistently [3].

3.7 Reverse Social Engineering

Trust is pre-established between the attacker and the victim. The attackers create a situation in which the victim requires help and then present themselves as someone the victim will consider someone who can both solve their problem and is allowed to receive privileged information. Of course, the attackers try to choose an individual who they believe has information that will help them [3].

3.8 Baiting

Is an attack during which a malware-infected storage medium is left in a location where it is likely to be found by the targeted victims [3].

3.9 Water Holing

Describes a targeted attack where the attackers compromise a website that is likely to be of interest to the chosen victim. The attackers then wait at the waterhole for their victim [3].

Table 1 – Classification of social engineering attacks according to our taxonomy.

		Phishing	Shoulder surfing	Dumpster diving	Reverse social engineering	Waterholing	Advanced persistent threat	Baiting
Channel	E-mail	✓			✓		✓	
	Instant Messenger	✓			✓			
	Telephone, VoIP	✓			✓			
	Social Network	✓			✓			
	Cloud	✓						
	Website	✓				✓	✓	
	Physical	✓	✓	✓	✓			✓
Operator	Human	✓	✓	✓	✓			✓
	Software	✓		✓	✓	✓	✓	
Type	Physical		✓	✓				✓
	Technical					✓	✓	
	Social				✓			
	Socio-technical	✓			✓	✓	✓	✓

Fig. 3. Classification of social engineering attacks [3].

4 Social-engineering Attack Risks

These are some of the greatest examples on how social-engineering attacks have damaged corporations, and brought to the frontline the notions of cybersecurity and its necessity. Not only the corporations are impacted, but also the people affiliated with these companies can have their data stolen. These are some of the risks a breach in security can have [11].

4.1 Yahoo Customer Account Compromise (2013)

Through a semi-privileged worker, 3 billion accounts were compromised, going up for sale on the dark web, being probably the biggest security breach ever [11].

4.2 Sony Pictures Hack (2014)

Due to a movie release satirizing North Korea, allegedly, north Korean hackers aimed to hurt the movie publisher, released several other pictures and a considerable amount of employee data online, making Sony suffer substantial financial losses [11].

4.3 Department of Labor Watering Hole Attack (2013)

A server of the Department of Labor was hacked, through a remote access Trojan named Poison Ivy. The hackers were never found, and it is hard to know the victims unless those victims come forward, because watering holes are websites or resources that look official but are traps set up by the attackers [11].

4.4 Ubiquiti Networks Scam (2005)

Attacker impersonated employees from the companies Hong Kong subsidiary, regarding instructions to changes in payment account details or new vendors to be credited, which, unverified, led to the $47 million in damages, recovering only $8 million, being the rest lost to the hackers [11].

4.5 RSA SecurID Phishing Attack

Attackers sent email with a spoofed address to four employees, purporting to be at a job recruitment website, with an Excel attachment. The files were opened, and a zero-day Flash exploit installed a backdoor access which stole the company's SecurID's two-factor authentications [11].

10.11228/dpsc.03.01.005

5 Prevention

The methods, motives and channels of attack are endless, and the battle between attackers and defenders is ongoing. “Most people do not realize just how much information they reveal about themselves, or the organizations that they work for, in the course of their daily discussions” [5]. The importance for cybersecurity is still downplayed, being the costs and complexity high, it is hard to insist on its importance. Sometimes, only when someone or a corporation is attacked, that the awareness. There are a wide range of tools nowadays to prevent against social engineering attacks, but despite these software applications, the number one factor to consider, is the human factor. To be well protected, one must first acknowledge the problem, “know thy enemy” and then act on the issue [12]. “The defense must have several layers of protection so that even if a hacker were able to penetrate one level, there would be other levels at which he/she would be stopped”, and this can be accomplished, among other things, by having software, human, and policy resources on the task [13]. There are three ways to defend against social engineering attacks, according to Douglas Twitchell: Education, training and awareness; Policies; Enforcement through auditing.

5.1 Education, training and awareness

It is not enough just to enforce policies and audit, because if the individuals aren’t taught why they must follow them, it remains hard to enforce it [14]. All staff must understand the necessity of cybersecurity at home and at work, especially when BYOD, and most importantly, their responsibility. Any breach can compromise their personal info or corporate info. This training should begin starting at employment all the way until the end of the employment. This training will make the individual aware of the risks, so he will be reluctant to disclose personal or corporate information, and be on the lookout and alert in case of social engineering signs like rushing processes, name-dropping, intimidation, small mistakes and requesting forbidden information or accesses. Another method could be having a website dedicated to security [12].

5.2 Policies

“The security policy sets the standards and levels of security that can be applied to any network, system or environment” [5]. The anti-social-engineering documentation’s standards cannot be unattainable. Must have a brief and concise list of what they should do, and not what they shouldn’t do, so they aren’t turned off by the policies, and don’t waste too much time reading [12]. Policies must be too reviewed regularly and stay relevant with the times, as security is constant evolving battle between attackers and defenders.

10.11228/dpsc.03.01.005

5.3 Enforcement through auditing

An audit is conducted internally or by a specialized entity, with the purpose of making a risk assessment, identifying the people involved, the hardware and software, vulnerabilities, risks, and plan countermeasures accordingly. “Any audit team has either the options to perform a full audit for all cybersecurity domains or by selecting specific domains to audit certain areas that need control verification and hardening” [15]. Auditing will have considerable impact not only in cybersecurity and data protection against hackers, but in increased performance, identifying gaps in the defenses, highlighting and addressing weak spots, delivering an in-depth analysis of internal and external security practices, adding reputational value to the company and assuring employees, clients and vendors [16].

6 Countermeasures

6.1 Use secure and complex passwords

A good password is a password that uses a mix of numbers, capital and lower-case letters, symbols and with no repetitive patterns as these can be cracked easily by brute force [12].

6.2 Use Two factor authentication

Something you have, something you are, and something you know. This is a method where various means are applied simultaneously that only the user has, is and knows, like a card and a password, or a card and a retina scanner [12].

6.3 Remove info from public information databases

The more information someone has on the Internet, the riskier it is. There are ways to disclose private information through previously uploaded data through sites like Facebook or Instagram that depend on their cybersecurity, so the least information you have, the safer you’ll be [12].

6.4 Monitor your data

Look for identity theft and credit card dubious movements. You need to be vigilant to breaches [12].

6.5 Never reveal passwords

Due to dumpster diving and shoulder surfing, it is easy to know someone’s password, but easier it is if someone knows your password. Don’t tell your password to anyone nor dispose of written passwords without destroying them [12].

7 Conclusion

The information gathered in this article was collected to bring awareness to the cyber-security paradigm. Not only as a study on social-engineering, but on the ways to prevent it, taking into consideration the various attack vectors, motives, phases and types of attacks, and acknowledging the results these breaches had in some of the greatest corporations in the world in the past. From all the new technologies and advances in software and hardware, the most vulnerable component and the one that cannot be changed is the human being. In order to “upgrade” the human factor, one must only learn and be aware, as it is the first barrier between being at risk and being safe. Only then can countermeasures be put into practice to protect from attacks. There are multiple ways to be attacked, and the inevitability of attacks is certain. Only one breach is needed to break a system, but all fronts must be protected.

10.11228/dpsc.03.01.005

References

1. Miller, K., Voas, J., Hurlburt, G.: Byod: security and privacy considerations. IT Professional 14(5):53-55 (2012).
2. Albladi, S., Weir, S.: User characteristics that influence judgment of social engineering attacks in social networks. Albladi and Weir Hum. Cent. Comput. Inf. Sci. (2018) 8:5.
3. Krombholz, K., Hobel, H., Huber, M., Weippl, E.: Advanced social engineering attacks. Journal of Information Security and Applications 22, 113-122 (2015).
4. Barbosa H., Breda F., Morais T.: Social Engineering and Cyber Security. International Technology, Education and Development Conference, DOI: 10.21125/inted.2017.1008 (2017).
5. Chantler, Alan and Broadhurst, Roderic: Social Engineering and Crime Prevention in Cyberspace. Technical Report, Justice. (2016).
6. Allen, M.: Social Engineering – A Means to Violate a Computer System. GSEC (2006).
7. Granger, S.: Social engineering fundamentals, Part I: hacker tactics. SecurityFocus. (2001).
8. Herley, C, Florencio, D.: Phishing as a tragedy of the commons. NSPW'08 (2008).
9. Nelson, R.: Methods of hacking: social engineering. http://www.isr.umd.edu/gemstone/infosec/ver2/papers/socialeng.html (2008).
10. Pais, R., Moreira, F., Varajão, J.: Engenharia Social (ou o carneiro que afinal era um lobo). Grupo Almedina: Pedro Campos e Pedro Quelhas de Brito (2013).
11. Cybersecurityeducationguides webpage, https://www.cybersecurityeducationguides.org/2017/11/top-5-social-engineering-attacks-of-all-time/ (2017).
12. Kumar, A., Chaudhary, M., Kumar, N.: Social Engineering Threats and Awareness: A Survey. Future Internet 11 (2019).
13. Gragg, D.: A multi-Level Defense Against Social Engineering. SANS Institute (2020).
14. Khonji, M., Youssef I., Andrew J.: Phishing Detection: A Literature Survey. IEEE Communications Surveys & Tutorials 15(4), 2091-2121 (2013).
15. Sabillon, R., Serra-Ruiz, J., Cavaller, V., Cano, J.: A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance. International Conference on Infor-mation Systems and Computer Science (2017).
16. Indusface webpage, https://www.indusface.com/blog/what-is-cyber-security-audit-and-how-it-is-helpful-for-your-business/ (2020/11/16).

SESSION 2
THE FUTURE OF RISK MANAGEMENT IN THE DIGITAL TECHNOLOGIES

Cybersecurity Risks on Automotive Industry

Bruno Rodrigues

Lúsofona University of Porto, Portugal
bfrodrigues15@gmail.com

Abstract. In plain twenty-first century, technology has exploded and exponentially grows everyday bringing innovation and commodity to the human being.
One aspect where technology was revolutionary was in the automotive industry. Themes like artificial intelligence supercharged cars with the capabilities that we know today. With innovation comes an increase in complexity and thus increases the concerns related with cybersecurity.
In this paper we will talk about the vulnerabilities and the effects that those have to the end consumer, also we will discuss some mitigation techniques that can be implemented both at manufacturing and software development level.
We will start by introducing the actual picture of the automotive industry and what advancements have been made till now. Here it will be discussed not only the actual techniques used and their vulnerabilities but also the reason behind such security threats in a world where we have achieved some high security standards.
Then will breakdown vulnerabilities in means of access (physical and remote). It will be described and explained the methodology applied to the different parts of an autonomous vehicle as well as some techniques and technologies that can help mitigate these vulnerabilities and contribute to a better and safer automotive future.
In the end will be presented a cyberattack example to round up the concepts discussed along the paper.

Keywords: Cybersecurity, Autonomous driving, Vehicles, Data Security, Communication

1 Introduction

Automotive industry has been revolutionizing herself lately. With the increasing advancements in technology, automotive brands started to adopt the benefits and the commodity that comes with terms like artificial intelligence consequence of the exponential growth when it comes to technological developments.

According to [1] “autonomous driving, connected cars, electric vehicles, and shared mobility have dominated the agenda of automotive industry leaders in recent years.

10.11228/dpsc.03.01.006

These innovations, built on the digitization of in-car systems, the extension of car IT systems into the back end, and the propagation of software, turn modern cars into information clearinghouses."

The main problem related with the increasing automation and "intelligence" of this type of vehicles is that to achieve this type level of complexity there is a growing need in adding lines of code. Every year cars get more complex and thus their ECU´s (Engine Control Unit) get a bigger number of lines of code. Has we know, every time we add code, we are increasing debug time and clearing room for possible vulnerabilities. Has stated by [2], "the average modern high-end car software is 100 million lines of code, to be compared with Windows 7 (39.5 million in 2009) or a Boeing 787 (13.8 million)."

This statement shows the complexity and the humongous amount of terrain to be covered by manufacturers and their counterparts.

This paper will focus on the "who" and "how" of those vulnerabilities and what improvements can we implement at the different manufacturing levels to achieve safer vehicles in the future.

On section 2 we will start by describing and contextualize the current picture in automotive industry.

On section 3 will be discussed sources of vulnerabilities and exploits on modern vehicles and some techniques to mitigate those vulnerabilities.

Then on section 4 we will see the importance of human behavior in cyberattacks success together with some examples that illustrate those same behaviors.

Finally, it will be presented an example of a real cyberattack to understand some of the concepts talked about along the paper as well as some recommendations regarding those vulnerabilities and exploits.

2 Current Picture in Automotive Industry

Today when we are looking for our next car, we look for some key aspects: fuel consumption, comfort, performance, and pleasure to drive.

These aspects are overrated by car manufacturers because these are the ones that sell their product. This is not a concern when it comes to the traditional vehicles but when we talk about cars with ever growing complexity when it comes to technology and automation, this can be considered a security threat. "This measure of quality is underpinned by regulatory activities that impose minimum standards for managing cybersecurity risks and require OEMs" (Original Equipment Manufacturer) "to have the ability to fix security issues via software updates." [1]

10.11228/dpsc.03.01.006

Nowadays the most used methodologies in automotive security practices are security management, penetration testing and dynamic security testing (DAST)[3].

According to a study made by [3], from all the participants that answered the study only (61 percent) apply security patch management and (56 percent) made penetration testing to ensure vehicle security. Figure 1 below exposes adoption rates for the various security practices used nowadays.

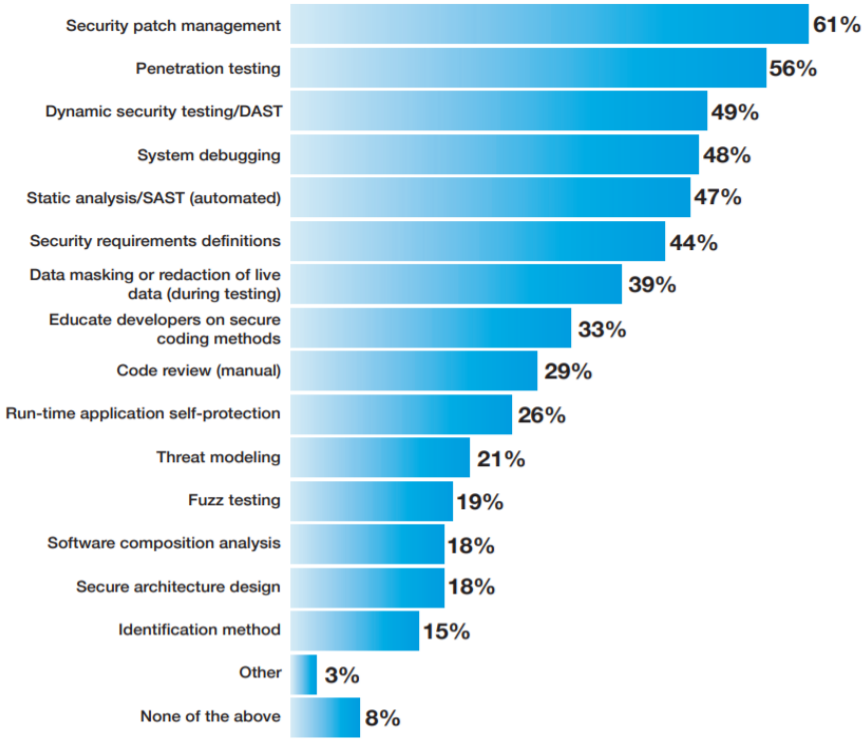


Fig. 1. - Adoption Rate of Cyber Security Practices in the Car Industry [3]

Secure architecture design stays at (15 percent) and code review (29 percent), two major steps to ensure a safe and less prone to breaches software. In contrast system debugging is quite high when compared with the previous two, sitting at (48 percent). This proves that the focus is on making it just work and ready from a consumer perspective, not making it work the right way by checking all the outcomes and variable in place.

This allows us to conclude the veracity of the statement made on the second paragraph on this section. Although there is plenty of countermeasures and practices that can reduce the risk of these vulnerabilities seems that manufacturers lack the ability to understand the need of investing in security.

3 Vulnerability Sources and Exploits

In this section we will breakdown vulnerabilities in current automated vehicles, but first let´s look at some factors that can increase the probability of these vulnerabilities being exploited:

- Implementation of software and hardware including apps, services and every form of communication offered by the vehicle
- Backend data and infrastructure which provide OEM firmware and OTA (Over-the-air) software updates
- Third party parts manufacturing and designing
- Driver behavior and knowledge

These factors will be described and broke down according to means of access in the next subsection:

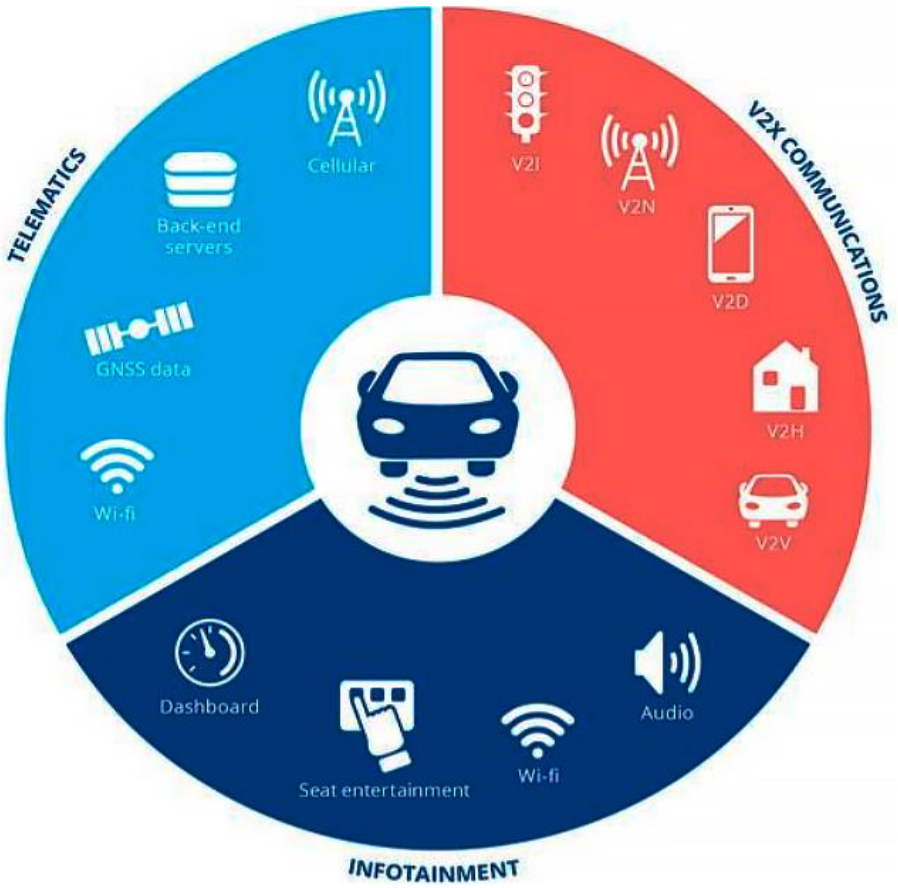


Fig. 2.- Smart Vehicles Ecosystem [4]

3.1 Physical Access Exploits

Physical access exploits have been one of the key aspects when it comes to whatever type of crime associated with vehicles. Along the years we have seen themes like theft and parts manipulation based on vehicle access and with the introduction of autonomous vehicles that vulnerability persists.

3.1.1 CAN (Controller Area Network) bus and ECU´s

Autonomous vehicles rely on CAN bus to control very important functions such as steering, acceleration and braking. This is considered the highest feasibility vulnerability at a physical access level since it controls the core aspects of a car.

A possible methodology of attack would be directly accessing the cables of the buses and manipulate them [5]. The risk underlying here sets on the nature of the ECU's and some of their purposes. One of the functionalities of this part is the capability of allowing service centers and authorized personnel to access the vehicle for diagnosis or modifications. Having direct access to the ECU's would allow hackers to have the same capabilities but with other intentions allowing for control over key functions of the vehicle.

Some examples of types of attacks achievable by targeting this unit:

CAN fuzzing attack-This attack bases itself in sending random data to CAN bus in [6]. The methodology sets behind listening and sniffing CAN messages over time.

CAN bus frame falsifying attack-This attack inserts incorrect data in CAN messages payload in order to falsify information [6].

CAN bus injection attack- Injecting data into a CAN bus can be used to send messages at an abnormal rate. "The purpose of this attack is to change frequency and amount of CAN frames."[6] This attack is achieved by manipulating vehicle´s decisions by overflowing the CAN bus with information.

3.1.2 Onboard Diagnostic ports

OBD or (Onboard Diagnostic) ports share a similarity with the methodology of attack described above. Here instead of physically manipulate the ECU and his counterparts the attacker takes advantage of the access to the service ports. By using these ports assigned to diagnose the vehicle during service, attackers can "eavesdrop on messages over these networks, send malicious messages, communicate with ECUs, and update ECU firmware using standard and low-cost off-the-shelf data logging and programming equipment."[7]

Such thing can be achieved by using the vehicles diagnostic port, if the target bus has pins that allow access to them, access can be achieved by swapping wires between the standard pins and target bus pins [8].

10.11228/dpsc.03.01.006

Methodologies to mitigate this type of attacks can be as follow:

- Parking vehicles in safe places and allow access only to authorized and trustworthy personnel [5]
- Implement software that monitors CAN inbound messages content and rate to detect abnormal behavior and control which messages are safe or not [5]
- "Implementing firewalls, whitelisting, and blacklisting of ECU messages to prevent unsafe commands" [5]

3.2 Remote Access Exploits

Most conventional cars nowadays have infotainment systems which allow to connect multiple devices to your car. Autonomous driving and connected vehicles are no different , in fact they are even more advanced in that matter. Unlike most of conventional vehicles, autonomous ones start to have OEM channels where telematic information and OTA software updates are available through those channels. All this connectivity allowance opens space for vulnerabilities at a remote level.

Now we will break down some common scenarios that explore vulnerabilities:

3.2.1 GPS and Cameras

This is considered a severe vulnerability when compromised since they are responsible for guiding the car. GPS tracks where the car is located at geographic level and camera reads the surroundings.

The most common exploitation on the GPS side is jamming. Here the attacker tries to falsify the location of the vehicle and provide wrong information to the driver. This type of attack is particularly difficult to detect due to environmental constraints.

When it comes to cameras, the methodology of the attack consists in blinding their vision. This can be made using high brightness IR LEDS or IR lasers [9].

This type of attack is on everyone´s reach since it uses components easily found online at a low price.

3.2.2 Onboard Sensors and devices

Onboard sensors can be incapacitated by an EMP (Electromagnetic Pulse) discharge. This type of attack generates an electromagnetic field to damage in-vehicle devices. Although this can be dangerous for the driver, not enough power can be generated to incapacitate a full vehicle [9].

Another type of attack is creating a ghost vehicle by using a digital radio frequency repeater, here the signal is replicated and retransmitted. Since this copy is very convincing the radar will interpretate it as an obstacle [9].

10.11228/dpsc.03.01.006

3.2.3 OTA Updates

Over-the-air updates are another source of vulnerabilities when it comes to remote access exploits. “remote OTA ECU firmware updates become increasingly important and expected, which increase the chances for malware to infect vehicles from remote sites.”[7] The attacker just needs access to the back-end server and from there it requests execution of an OTA firmware update for a fleet of vehicles [4].

After that the process is just like a normal firmware update where the user accepts it and then the hacker uploads the modified firmware update which contains a backdoor and from that point on he has now access to the vehicles that installed that modified firmware [4].

3.2.4 Vehicle Infotainment

In-vehicle infotainment systems present multiple connection resources like Bluetooth, Wi-Fi, Zigbee or universal serial bus [9].

Most of these systems are based on well-known distributions that we use on our computers. This familiarity with operating systems like Linux, Green Hills, Windows CE, and QNX, allowing hackers to implement and reuse the knowledge that they already have from computers [5].

Other key aspect is reutilization. Manufacturers want to use software in as much vehicles as they can so that is easier to maintain and reduce costs on development which takes the same vulnerabilities to a wider range of vehicles.

Methodologies to mitigate this type of attacks can be as follow:

- Require authentication for both the user, OTA updates and services that directly influence important parts of the vehicle so integrity and availability can be maintained on core services and functionalities of the vehicle [5].
- Run infotainment communications on a different channel from the one that handles all the data related with operations and safety management [5].
- Encrypt OTA updates and allow to reverse them in case of a severe security breach [5].

4 Human Behavior and Vehicle Cyberattacks

Despite all the vulnerabilities and methodologies described in this paper, there is one more key intervenient when it comes to cyberattacks in vehicles and their success.

Drivers are one the most vulnerable parts on a vehicle cyberattack simply because is very easy for hackers to get access to the car by luring the driver into doing some type of action that triggers malware or other type of malicious implementation.

10.11228/dpsc.03.01.006

This is one of many examples of an ever-growing source of cyberattacks, social engineering. Simple events that at first site seem unharmful like opening a link sent through an email or message or opening a suspicious website can lead to malware injection in the same way it happens in our laptops, phones, and such. After all current autonomous vehicles are real computers where you can do everything that you would normally do on a laptop.

All the scenarios talked above are possible because of human behavior and lack of cybersecurity awareness.

Risky cybersecurity behavior is connected to the over-trust of automated technologies. "When the driver trusts their car too much, it is more prone to attack."[10][11] This happens because people misunderstand or are not well informed about the limitations of an autonomous driving vehicle or simply because they use technology on a daily basis and think they know all about it.

4.1 How Behavior Patterns and Skills Affect Vehicle Cyberattacks Sucess

Numerous studies have been made related with the relationship between human behavior and vehicle cyberattacks. According to those studies "people are prone to behaving in a more risky fashion towards cybersecurity if they are more extraverted, addicted to the internet, impulsive, and less conscientious." [10][12]

This fact allies to other human behavior variables such as the capability of assess a problem, reacting under pressure and multitasking. The capacity of problem assessment varies from people to people, "23% of people correctly handle less than half of cybersecurity scenarios; only 4% can handle more than 90% of scenarios." [10][13]

Other aspect is distraction. This one is common to automotive industry in general, nevertheless distraction plays a major role when it comes to abnormal behavior detection. Paying attention to other events or multitasking can prevent, for example, the driver from reacting to an unexpected turn caused by a remote attack.

Distraction can be paired with capability of reacting under stressing circumstances. An unexpected switch in a car behavior can make the driver stress and thus affect his decision capability leading to disaster. An attack success rate increases when the driver realizes he is not in control anymore, here the driver starts behaving irrationally and making untaught judgements opening space for unwanted events [10][14].

What was described in this subsection represents another source of cybersecurity vulnerability, one that is more abstract since it depends on the human mind. Nevertheless, manufacturers should invest in awareness as a way to mitigate cyberattacks since the driver plays such an important role in preventing them as we saw.

5 Jeep Cherokee Hack - A cyberattack Example

Now we are going to discuss an experiment presented in [15]. The objective with this discussion is to understand how the vulnerabilities and exploits talked above are explored in a real situation with a vehicle. Although the vehicles targeted in this study are not autonomous, the principle behind it remains the same.

We will start by describing which parts of the vehicle were explored to conduct the different types of attack achieved in the experiment.

- Explore infotainment system WIFI connection
- Exploring the link between CAN bus and a V850 Controller (cellular network)

The first type of attack consists of exploring the hotspot WIFI feature present in the infotainment system. The problem with this approach for who wanted to hack the vehicle were two factors.

First hotspot Wi-Fi is a paid service which on a long run would be costly for most people so it wouldn´t target a big audience, second you would still need to figure out the WPA2 password to connect to Wi-Fi which will be discussed next.

Now let´s take a look at the way WPA2 passwords are generated.

The system presents in the vehicles used in this study calculated the password by using the time/date which normally is acquired through the v850 controller by cellular network, so it is similar to the way our phones acquire the same time and date. The problem is that at boot time the system does not know time/date yet, so it uses a default time plus the time Wi-Fi service takes to boot. The combination of these two variables give us the password of the device, then you just need to convert it to UNIX epoch time, and you have the WPA2 password.

Obviously, the way passwords are generated makes it easy to guess since it results on a relatively small number of combinations if we would use a brute force attack. Experts estimate that it could take as low as one hour to discover the password through a brute force attack.

The focus of the attack relies on a specific TCP (Transmission Control Protocol) active port, the one used by D-bus. D-bus is an inter process communication mechanism that handles the data share between processes.

This mechanism allows to have access to the services and methods used to control several aspects of the infotainment and other features like ac and radio. Normally this D-bus has authentication implemented so that only authorized credentials can have access to those services. Nevertheless, Jeep didn´t have any authentication constraints so you could just declare yourself as Anonymous and have access to everything inside it. This

added to the fact that D-bus ran as root would allow to execute any commands with administrator privileges if a shell could be used.

5.1 D-bus Command Line Injection

Now that they granted access to all services, they had access to all services, during their research they found one service in particular that had a vulnerability, this vulnerability allowed the execution of any line of code or instruction that we wanted including changing volume or ac temperature. From this point on , they had access to the vehicle head unit where they could control every aspect except car essentials such has braking and steering.

5.2 Connection to CAN bus: The Challenge

So, until now, access to infotainment system has been totally granted, but the way it was designed prevents the infotainment system from connecting directly with the CAN bus so that the infotainment system cannot control physical parts of our vehicles such has steering.

Nevertheless, experts found that another unit, the v850 controller actually connects directly with the CAN bus. Although originally this was designed not to allow execution of code, just listen to CAN bus. This limitation was overridden has we are going to see later on.

Now that they knew the relationship between the v850 module and the CAN bus it was time to access this unit trough cellular network because not everybody would pay for hotspot WIFI connection, so that methodology was only useful to a minority of cases.

In order to do that experts bought femtocells which they used to connect a phone with cellular data from local carrier to the car. This allowed them to list IP addresses on the network and also find, not only the local IP address of the car they had, but multiple cars connected to the same carrier.

5.3 V850 Firmware Flashing

So up until moment experts were not still capable to connect to the CAN bus and actually affect the physical parts of the vehicle. So, the solution was to turn the attention to the v850 chip. The v850 chip was the only component accessible externally that had contact with the CAN bus.

In order to get over this limitation experts wrote their own version of the v850 controller firmware and flashed it.

Since once again firmware packages are not signed and flashing them did not require a signature either all they had to do was reflash the v850 controller with their firmware.

By flashing modified firmware to the v850 chip they overcame the initial challenge of sending messages to the CAN bus.

Now all that was left was to send shell commands to control key functions of the car such as steering, proximity sensors and such.

5.4 What can we take from this cyberattack?

This cyberattack is an example of the lack of investment in security by car manufacturers.

There were some barriers and security concerned design in some aspects till some extent. Nevertheless, a lot of vulnerabilities were found, and shortcuts were taken.

Some ways of improvement would be increasing the complexity of Wi-Fi WPA2 passwords generating algorithm, using a hash function to generate a unique signature to validate firmware updates and fix memory corruptions. These are some of the improvements that could be implement in first place.

Is also important to have in mind that to execute this attack physical access and time were needed. Firmware flashing involves a USB stick and direct interaction with the vehicle infotainment making this attack more difficult. Still, this vulnerability was present in approximately 1.4 million vehicles.

This proves the importance of manufacturers investing in safer methodologies and implementations as cars automation and complexity grows. The cult of a laid-back approach from manufacturer side resulted in many other studies and cyberattacks that happened exactly by the same reasons.

Luckily, most of this cyberattacks are not harm targeted and so we can learn more about how they happen and how to mitigate them.

6 Conclusion

Along this paper we presented numerous vulnerability and exploitation sources. These vulnerabilities and exploitations are the result of administrative decisions, priority hierarchy, software development lifecycle nature and security awareness between car manufacturers and their counterparts.

Nowadays security has evolved, and some manufacturers already see it has a threat and a feature worth investing. Nevertheless, there is still plenty to do, mainly when it comes to awareness and build the importance of security in people´s mind. Only that way we will end with laid back approaches both at manufacturing level and software development wise allowing vehicle industry and technology to grow together.

With the increase of customer awareness, new methodologies of mitigation and studies are in the works, futureproofing the viability of the ever-growing technology influence in vehicles.

This is a great opportunity to revisit and forward develop this subject evaluating which new threats evolved and how those are being threated, compare it with the current situation and even develop a case study based on those aspects.

7 References

1. Mckinsey and Company, "Cybersecurity in automotive-Mastering the Challenge", (2020)
2. Altran, "Cybersecurity in Automotive-How to Stay Ahead of Cyber Threats", (2018)
3. Ponemon Institute, SAE International, Synopsys , “Securing the Modern Vehicle Practices: A Study of Automotive Industry Cybersecurity Practices”, (2018)
4. ENISA,“Enisa Good Practices for Security of Smart Cars”, (2019)
5. Hodge, Cabell, Konrad Hauck, Shivam Gupta, and Jesse Bennett. “Vehicle Cybersecurity Threats and Mitigation Approaches.” Golden, CO: National Renewable Energy Laboratory. NREL/TP-5400-74247, (2019)
6. Emad Aliwa, Omer Rana, Charith Perera, Peter Burnap, “Cyberattacks and Countermeasures for In-Vehicle Networks”, (2020)
7. Zhang T., Antunes H., Aggarwal S., Defending Connected Vehicles Against Malware: Challenges and a Solution Framework. IEEE Internet of Things Journal. 1, (2014)
8. Aastha Yadav , Gaurav Bose , Radhika Bhange , Karan Kapoor , N.Ch.S.N Iyengar , Ronnie D. Caytiles,” Security, Vulnerability and Protection of Vehicular On-board Diagnostics”, *International Journal of Security and Its Applications Vol. 10, No. 4*, (2016)
9. Jonathan Petit, Steven E. Shladover, "Potential Cyberattacks on Automated Vehicles", (2014)
10. Václav Linkov, Petr Zámečník, Darina Havlíčková, Chih-Wei Pai, “Human Factors in the Cybersecurity of Autonomous Vehicles: Trends in Current Research”, (2019)
11. Parkinson S., Ward P., Wilson K., Miller J.,”Cyber threats facing autonomous and connected vehicles: future challenges”, *IEEE Trans. Intel. Transport. Syst.* 18, (2017).
12. *Hadlington L Heliyon,“* Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours”*,* (2017)
13. Yan Z., Robertson T., Yan R., Park S. Y., Bordoff S., Chen Q, “Finding the weakes links in the weakest link: how well do undergraduate students make cybersecurity judgment? *Comput. Hum. Behav.* 84”, (2018)
14. Moisan, F. and Gonzalez, C ,”Security under uncertainty: Adaptive attackers are more challenging to human defenders than random attackers”, Frontiers in Psychology, 8:982, (2017)
15. Charlie Miller,Peter Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle”, (2015)

Estimating the Cyber Risk of the Financial Sector in Portugal

José Barbosa

Lusófona University, Porto - Portugal
josepmbarbos@gmail.com

Abstract. In a world where technology has taken over most aspects of our daily lives, the financial sector is not an exception. In the same way that our information and data can be stolen, intercepted or even tampered with, the financial sector is subject to a much higher cybersecurity risk than any other sector. From banks to the stock market, even insurance companies, no one in this sector is immune to attacks in the technological department. On this paper, we will be focusing on the cybersecurity threats to the financial sector worldwide, and then we will focus on the case of Portugal. We will also discuss the risks, vulnerabilities and the means to prevent attacks and intrusions to promote cybersecurity.

Keywords: Technology, Financial sector, Cybersecurity risk, Stock market, cybersecurity.

1 Introduction

With the invention of the computer and the exponential technological advances that followed it, most industries and services were able to implement such advancements, that provided them with certain advantages such as the automatization of certain tasks and serving as an aid in others. These advancements proved themselves incredibly useful.

They were followed by another invention that would change the way we go about our daily lives, a way to connect all our computers and many of our devices, the internet. With an impact reminiscent of the industrial revolution, these new discoveries launched us into the cyber era and changed business and life altogether.

One of the biggest profiteers of these technological advancements was the financial sector in general. From banks, ATM's (Automated Teller Machine) and even the stock market all relies on cutting edge technology. [1] [2]

With these new opportunities, came new means of to carry out criminal activities, relying on the communication between these systems. Either for espionage in order to gain advantage over the competition or even theft, given that these systems handle monetary transactions, with the digitalization of the financial sector, a door was opened for those with knowledge and criminal intentions, making these new advancements as damaging as they are rewarding. [3]

10.11228/dpsc.03.01.007

2 Cybersecurity threats to the financial sector

2.1 Definition of the financial sector

The financial sector is a section of the economy made up of firms and institutions that provide financial services to commercial and retail customers. This sector comprises a broad range of industries including banks, investment companies, insurance companies, and real estate firms. [4]

2.2 Cybersecurity threats that target the financial sector

Being one of the biggest sources of income in multiple countries, the financial and the insurance industry are also one of the most desirable targets for hackers and cyber criminals [5]. For this reason, this sector is subject to several threats, such as:

- **Malwares**: short for malicious software, a malware consists of a harmful computer program that aims to get access to privileged information. A malware is essentially a program design to cause harm to a system and can do so in several ways [6]. In this case, it is common the use of information stealing malwares, such as key loggers able to steal passwords [5].
- **Phishing**: phishing consists of a fraudulent message, in form of a text message or an email, that tries to trick the receivers into believing that they are going to win something or that they have debts to pay, and will try to convince them to download an attachment or click on a link. What makes these attacks particularly effective is the fact that the attacker disguises himself as someone who the victim trusts or might even do business with. It is one of the oldest forms of cyber-attack [7]. This results in the disclosing of financial and personal information, identity theft, identity fraud and theft of personal information [5].
- **Theft or loss of proprietary or confidential information or hardware**: A data breach, harmful to the company who suffered it both financially and in terms of reputation, that can be divided into two categories, physical breaches, when using, for example, stolen data storage devices, and non-physical breaches, such as network intrusions [5].
- **Insider abuse of access**: This happens when someone who has authorized access, use their knowledge of the business's vulnerabilities to carry out illicit or malign activities, such as theft, eavesdropping, modification of information or even for their personal advantage by selling the information to the competition or using it for their personal advantage [5].
- **Denial-of-service**: The denial-of-service consists of an attack directly upon the computer or system that one aims to render useless. These attacks are made by flooding a system with requests, making it so that normal traffic cannot be processed, thus denying services to its users. These can be divided into two categories, buffer overflow attacks, which is when an overflow consumes all the hard disk space, memory, or even CPU time,

and flood attacks, when a designated server is flooded with packets, thus saturating the server, and rendering it useless [8].

2.3 Measures to prevent cyberattacks

Within the financial sector and when it comes to cybersecurity threats, attacks share one of two natures, being either internal or external.

The internal attacks are known to be more dangerous and damaging, and according to the 2014 U.S. State of Cybercrime Survey [10], 37% of organizations have suffered an insider attack and 32% go as far to say that these attacks were more damaging than the outsider attacks. In 82% of the cases, sensitive or private information was released to the public unintentionally and in 72% of the incidents, confidential data was stolen. In 71% and 63% of these incidents, respectively, customer and employee records were compromised or stolen.

These numbers, while worrying, are only referring to the known cases of insider attacks, since most of these transgressions usually go unnoticed. They are mostly handled internally and very rarely they involve legal actions, mostly due to the lack of evidence usually attributed to these cybercrimes and the difficulty to prove malicious intent. [9]

These attacks happen mostly due to lack of awareness and the negligence of basic security measures such as password sharing practices, unlocked devices, unsecure Wi-Fi networks and weak passwords.

Some of the best ways to prevent insider attacks are:

- **Educating employees –** By showing employees the importance of cybersecurity and the correct practices, resources and measures for safe networking.
- **Encrypting data –** Making our data unreadable and useless to those who access it without permission.
- **Implementing proper password managing practices -** Enable two-factor-verification and use complex passwords to add a second layer of security and reconfirm a user's identity every time they log in. Change passwords every six months and make sure they contain upper and lowercase letters, numbers and symbols.
- **Installing antivirus software –** Antivirus scan the whole system in search of malicious files or even virus and in most cases can even handle spyware and malware.
- **Updating all devices –** Outdated devices are usually more vulnerable to all types of unauthorized accesses. [11]

Outsider attacks however are when individuals or group tries to steal protected data or more, by infiltrating the system or organization in question. They can be individual hackers, organized crime groups or even government entities. The attack itself can also be divided into active or passive. An active attack generates packets or participates in the network while a passive attack is eavesdropping the network or tracking users. The motive behind these attacks can be Cyber Espionage, Cyber Warfare, and Hacktivism. [12]

The following measures may reduce the risk of suffering an outsider attack:

- **Using multi-factor authentication –** This system makes it so that more than one factor is required to access our data. If the only mean of protection we have is a password, it can easily be compromised through phishing attacks for example. If the system is protected with more than just a password, but also a card, or an email verification it becomes harder to access it without authorization.
- **Responsibilities of third-party security –** if it is crucial that third parties must access our systems, such as vendors or other companies, it must be done in a safe way. In this case, it is necessary to monitor the networks, creating tight security controls and to identify potential cyber threats.
- **Educating employees –** this measure is important for both outside and inside threats. Employees may be victims of scams, phishing attacks or many other schemes, that may be avoided if they are prepared to face such issues. This can be done through seminars, or even annual training sessions.
- **Creating data backups –** creating data backups is essential to assure that the business in question maintains its productivity, even in the wort case scenarios. this prevents us from losing our data and even helps with some ransomware cases.
- **Keeping the systems updated –** Outdated systems are usually easier to access. For this reason, keeping the systems updated, even if there is some financial cost attached to it, is crucial to the security of the business. Updates patch vulnerabilities that previous versions might have had and protect against potential security threats.
- **Installing antivirus and firewalls –** Possibly the most important step in what comes to protection from outside attacks, is to install antivirus software in every system that accesses the private network of a business and regularly update it. And for further protection a firewall should also be installed, in order to prevent threats from the outside. [13]

3 The cyber risk to the financial sector in Portugal

3.1 Financial institutions in Portugal

According to a study by Banco de Portugal [14], in 2018, financial institutions were the victims of 25,7% of all malicious cyberattacks, in the first three months of 2019, the number of credit card thefts increased by 212%. There was an increase of 129% of client's credentials being compromised and there was an increase of 102% of malicious apps, including bank related apps for mobile devices.

In a country where the financial sector grows daily, cybercrime is still one of the most damaging factors to the economy, almost as much as geopolitical uncertainties and NPL's (Non-Performing Loan).

Figure 1 – The growth of cybersecurity risk as a concern to the global economy. [15]

Cybersecurity incidents may be responsible for the following impacts:

- **Financial risk –** Cybercrime results in major monetary losses, it may involve judicial costs, expropriation of funds, the costs associated with the safety of the damaged systems and taxes or sanctions for non-compliances of contractual obligations.
- **Reputational risk –** Companies and service providers will lose the trust of their clients for the mediatic exposure associated with security issues. The non-compliance of security measures may lead to sanctions and even further defamation of the business in question. Critical data may also be exposed to the public.
- **Operational risk –** The company may be unable to provide essential services to the public. Inability to integrate systems and networks in outsourcing.
- **Legal risk –** Non-compliance of deadlines, inability to comply with legal and contractual obligations. Inability to obey the AML/CTF (Anti-Money Laundering, Counter-Terrorism Financing) legislation. Loss of data integrity and confidentiality. Possible occurrence of disputes.

10.11228/dpsc.03.01.007

These risks all lead to monetary lost and to the disruption of services, and all may lead to financial instability.

Due to growing threat of cybercrime, Portugal has qualified authorities that assist those who have been victims of these crimes. The CNCS (Centro Nacional de Ciber Segurança), is the national centre of cybersecurity, and is the entity to whom all types of cybercrime must be reported by law. And the UNC3T (Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica), the operational unit that helps prevent and overall fight cybercrime. This unit handles prevention, detection and investigation of cybercrime.

Banco de Portugal divides authority approach in three fundamental pillars:

- **Regulation**
- **Supervision**
- **Cooperation**

3.2 Report obligations

If a financial institution was to fall victim of a cybercrime, the incident must be reported to legal authorities. Once it occurs, we must evaluate first if its impact was relevant. In order to evaluate it, we must answer questions such as:

- How many users did it affect?
- Was it damaging economically?
- Was it damaging towards the business' reputation?
- Did it activate the crisis management mechanisms?
- Was it attributed internal relevance?
- Were there any legal or regular non-compliances?
- Is it a systemic risk?

By answering these questions, we can determine if an attack was relevant or not. If the attack was considered relevant, it should be reported to the CNCS in three phases:

- **Initial (< 2 hours)** – A brief notification and description of the attack.
- **Intermediate (< 10 days)** – Details and relevant actualizations.
- **Final (> 30 days)** – Causes and corrective measures applied.

If the attack wasn't relevant however, then, the CNCS does not need to be informed of the transgression or should be notified voluntarily. [14]

4 Denial of Service (DoS)

A denial of service attack is a type of cyber-attack where a malicious individual or group tries to render a computer or any other system unavailable and therefore, useless to its intended users by interrupting the device's normal functioning. They usually function by flooding or overwhelming the targeted system with requests until normal traffic can no longer be processed, resulting in denial of service to the users. In a DoS attack only one computer is used to start the attack. These attacks usually target the infrastructure layer; however, they may also target the application layer.

Another attack of the same nature as DoS is the DDoS which stands for distributed denial of service. It consists of a DoS attack that comes from multiple sources.

DoS attacks are usually divided into two categories:

- **Buffer overflow attacks –** It is an attack in which a memory causes the system to consume all available hard disk space, memory or CPU time. This attack usually results in system crashes, sluggish behaviour and other inconveniences that ultimately lead to denial of service.
- **Flood attacks –** These attacks work by saturating a targeted server with an overwhelming number of packets, saturating server capacities, and causing denial of service. For these attacks to work, the attacker must have a wider bandwidth than the victim.

Some of the biggest DoS attacks so far have been:

- **Smurf attacks –** Attacks where an individual utilizes the broadcast address of a vulnerable network by sending spoofed packets resulting in the flooding of the targeted IP address.
- **Ping flood –** A simple form of DoS is based on flooding the target with ICMP (ping) packets. By feeding the target more pings than it is able to respond, we may cause denial of service. This attack can be qualified as a DDoS.
- **Ping of death –** Often confused with ping flood, the ping of death consists in sending the targeted system a malformed packet, that results in harmful behaviour, such as system crashes. [16]

4.1 Real cases of DoS in the financial sector

On September and October 2012, a group by the name "Izz ad-Din al-Qassam Cyber Fighters" attacked several financial institutions. On December that same year, the group attacked six banks in three days, by causing severe slowdowns and blocking access to the banks. Luckily, the previous attacks encouraged banks to prepare themselves for future attacks, thus making the attacks less impactful than they might have been. [17]

More recently, a series of Hungarian banks and telecommunication companies were also attacked by powerful DDoS attacks, launched from servers in Russia, China and Vietnam. [18]

4.2 How to prevent DoS attacks

In order to reduce the risk of suffering a DoS attack, the following measures should be implemented:

1. **Reducing the area of the attack surface –** By minimizing the surface that can be attacked, we limit the attackers' options and allows us to focus our protection in one place. We do this by making sure that our devices don't communicate with doors, protocols or apps that are not supposed to communicate with it.

2. **Planning –** The two main aspects that should be planned are bandwidth and server capacity. In terms of bandwidth, we must make sure that the provider offers a broad connectivity that can handle great volumes of traffic. In what comes to the server capacity, since DoS attacks are meant to consume resources, it is important that we can control our resources when needed. We do this by running larger computing resources or those that have features like more extensive network interfaces or enhanced networks that support larger volumes.
3. **Knowing the difference between normal and abnormal traffic –** Whenever an excessively large amount of traffic is detected, the host must process it without affecting the system's availability. Advanced protection techniques are able to accept only the legitimate traffic by analysing individual packages.
4. **Implementing firewalls –** Firewalls can protect us from all sorts of attacks, namely SQL injection or request forgery between sites, which attempt to exploit a vulnerability in the application itself. Firewalls can filter packages by country, by size or even IP, which makes us able to choose the traffic that we will receive.

5 Conclusion

Without any doubt, the market and industries will continue to grow with the aid of networking and technology in general. The exponential evolution we've gone through over the last decades brought over numerous advantages but on the other side, it also cursed us with other ways to damage, steal or harm us.

The financial sector is no exception, as it is the sector that is the most subject to all cybersecurity threats, whether they come in the form of unauthorized accesses, phishing scams or even the much-dreaded DoS attacks.

While writing this paper I gained a more serious notion that cyber security is not just something that is advised, it is essential in order to safely benefit from all types of networking, namely when handling monetary transactions or large monetary amounts.

References

1. R. Gourlay, A., J. Pentecost, E.: The Determinants of Technology Diffusion: Evidence from the UK Financial Sector. Economic Research Paper No. 00/9. (2000).
2. Lagazio, Monica, Sherif, Nazneen and Cushman, Mike (2014) A multi-level approach to understanding the impact of cyber crime on the financial sector. Computers & Security, online . pp. 1-32. ISSN 01674048 (In Press)
3. ERIKSSON, J., GIACOMELLO, G.: The Information Revolution, Security, and International Relations: (IR)relevant Theory?. International Political Science Review. 27, 221–244 (2006).
4. Kenton, W.: Financial Sector, https://www.investopedia.com/terms/f/financial_sector.asp.

5. Choo K 2011. Cyber threat landscape faced by financial and insurance industry. *Trends & issues in crime and criminal justice* no. 408. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi408
6. Fruhlinger, J.: Malware explained: How to prevent, detect and recover from it, https://www.csoonline.com/article/3295877/what-is-malware-viruses-worms-trojans-and-beyond.html.
7. Fruhlinger, J.: What is phishing? How this cyber attack works and how to prevent it, https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html.
8. What is a Denial-of-Service (DoS) Attack?, https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/.
9. Kul, G. and Upadhyaya, S., 2020. Towards A Cyber Ontology For Insider Threats In The Financial Sector. State University of New York at Buffalo, Buffalo, NY, USA.
10. C. I. T. Center, "2014 U.S. State of Cybercrime Survey," July 2014.
11. Grinavich, J., n.d. Business Security: How To Prevent Insider Attacks. [online] Vector Security. Available at: <https://www.vectorsecurity.com/blog/business-security-how-to-prevent-insider-attacks> [Accessed 16 December 2020].
12. JA, A., 2015. Insider Vs. Outsider Threats: Identify And Prevent |. [online] Resources.infosecinstitute.com. Available at: <https://resources.infosecinstitute.com/topic/insider-vs-outsider-threats-identify-and-prevent/> [Accessed 17 December 2020].
13. Managed IT Services & Technology Consulting | OSIbeyond. 2020. How To Prevent Cyber Attacks On Businesses In 2020 | Osibeyond. [online] Available at: <https://www.osibeyond.com/blog/7-methods-to-prevent-cyber-attacks/> [Accessed 17 December 2020].
14. Costa Ferreira, L., 2019. Ciber-resiliência no setor bancário A perspetiva do Banco de Portugal.
15. Lagarde, C., 2020. Estimating Cyber Risk For The Financial Sector. [online] IMFblog. Available at: <https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/> [Accessed 18 December 2020].
16. Cloudflare. 2020. What Is A Denial-Of-Service (Dos) Attack?. [online] Available at: <https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/> [Accessed 18 December 2020].
17. Felter, B., 2020. 7 Of The Most Famous Recent Ddos Attacks. [online] Vxchnge.com. Available at: <https://www.vxchnge.com/blog/recent-ddos-attacks-on-companies> [Accessed 18 December 2020].
18. Carnegie Endowment for International Peace. 2020. Timeline Of Cyber Incidents Involving Financial Institutions. [online] Available at: <https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline> [Accessed 18 December 2020].
19. Amazon Web Services, Inc. 2020. O Que É Um Ataque Ddos E Como Proteger Seu Site Contra Um Deles. [online] Available at: <https://aws.amazon.com/pt/shield/ddos-attack-protection/> [Accessed 19 December 2020].
20. B. Panja, D. Fattaleh, M. Mercado, A. Robinson and P. Meharia, "Cybersecurity in banking and financial sector: Security analysis of a mobile banking application," *2013 International Conference on Collaboration Technologies and Systems (CTS)*, San Diego, CA, 2013, pp. 397-403, doi: 10.1109/CTS.2013.6567261.
21. *Catota, F., Morgan, M. and Sicker, D., 2018. Cybersecurity incident response capabilities in the Ecuadorian financial sector. Journal of Cybersecurity, 4(1).*

22. *Journal of Xidian University, 2020. The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector. 14(7).*
23. *Didenko, A., 2020. Cybersecurity regulation in the financial sector: prospects of legal harmonization in the European Union and beyond. Uniform Law Review, 25(1), pp.125-167.*
24. *Calliess, C. and Baumgarten, A., 2020. Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective. German Law Journal, 21(6), pp.1149-1179.*
25. *Smith, S., 2020. EMERGING TECHNOLOGIES AND IMPLICATIONS FOR FINANCIAL CYBERSECURITY. International Journal of Economics and Financial Issues, pp.27-32.*

Complexities and Evolutions in Forensic Analysis of Mobile Applications

Tiago Daniel dos Santos Martins [0000-0002-4308-9821]

University Lusófona of Porto, 4000-098 Porto, Portugal
tiagomartins98@gmail.com

Abstract: Smartphones have become a standard in modern times, almost everyone has one, and some even require one to do their work. These devices have much personal information on them. They can have anything from our text messages, call records, bank logins, and any other accounts that we use, be it from a social network or otherwise. In recent years, as technology evolved, we started noticing a rise in privacy concerns and security features. As a result, mobile application forensics has become increasingly complex, and the trend shows no slowing down in sight. The implementation of encryption on storage or communications, more strict permission systems, and protected system partitions makes the forensic process more complicated and time-consuming. Forensics is a vital part of law enforcement work because, many times, it is necessary to analyze the device of a suspected criminal as part of the investigation. The purpose of this paper is to evaluate how mobile application forensics has evolved and what complexities can arise from the process. Firstly, we will review the steps of examining a device, what methods the analysts use, and each one's advantages and disadvantages. Finally, we will evaluate how this process has changed, what complications have emerged from security measures implemented by device manufactures or users, and what strategies were created by analysts to overcome these problems.

Keywords: Smartphones, Mobile Applications, Forensic Analysis, Technical Complexities, Forensic Techniques Evolution.

1 Introduction

Mobile forensics, a digital forensics branch, is defined as the science of recovering digital evidence from mobile phones under forensically sound conditions using accepted methods [1].

10.11228/dpsc.03.01.008

Table 1. Number Of Smartphone & Mobile Phone Users Worldwide (Billions) [2]

Year	Number of smartphones	Number of mobile phones
2019	3.2	4.7
2018	2.9	4.6
2017	2.7	4.4
2016	2.5	4.3

As we can see in the table above (Table 1), there are many phones globally, but we also use them for everything. They became our preferred way of digital communication [3]. We make calls, send text messages or instant messages, take pictures, record video or audio, read email, browse the news, login into our bank, the list goes on forever. When dealing with smartphones, besides de data on the device itself, it is almost sure that we might leverage some credentials to access further information stored in the cloud, like social media or email accounts. Maybe cloud storage was syncing with the device [4].

This data can usually be recovered and analyzed to redact a report, summarizing the recovered information more comfortable to read and accessible format [1]. The recovered data is crucial for law enforcement, as it can be useful in an ongoing investigation or as evidence in a court of law. As with other forensics procedures, specific guidelines and conditions must be fulfilled for the data to be considered valid evidence [1],[5].

Previously, obtaining the device's data was easy. The first generations of mobile phones had practically no security measures, and permission systems were lax. Nowadays, it is a whole different story [6]. Nowadays, device manufactures have implemented file-based encryption [7], sometimes even full disk encryption [8], more restrictive permissions [9], complex password requirements, fingerprint readers, and many more security and privacy-related features. There is also a plethora of new applications for communication with enhanced security features, as opposed to the classic text message or phone call [10],[11],[12].

To better understand how mobile forensics works and how it evolved to overcome new problems, we will examine the procedures involved in smartphone forensic analysis. We will talk about the necessary steps, the different methods available, and the guidelines to ensure that our data is valid. After we understand how it all works, we will review what complications have appeared in recent years, how they affect the forensics process, and what solutions have analyst came up with to overcome them.

2 The Forensic Analysis of Smartphones

2.1 Device Seizure

There is a crucial moment in smartphone forensics before the device even reaches the lab. When the court issues a warrant, law enforcement detains the suspect and immediately confiscates any electronic devices called a seizure [13]. The devices are physically seized and isolated from any radio signal, mainly if found in an on-state during a raid [4].

10.11228/dpsc.03.01.008

The objective of isolation is to preserve as much evidence as possible from the device. We accomplish it by blocking network access to prevent network-related anti-forensics countermeasures implemented by the suspect [1] or any data from being overwritten [14]. There are a variety of isolation methods, but these three are the most popular ones:

- Enabling "Airplane Mode" – requires physically interacting with the device. Therefore, it is not always an option, and we also risk losing data or locking the device because of some security measures put in place by the owner [1].
- Turning off the device – will block it from connecting to any network, but there is a very high chance that it locks the device [1].
- Faraday containers – using these is the best option, as we are not required to interact with the device. They use a unique material that attenuates, not block, radio signals, but they deplete the battery faster [1].

These isolation measures are temporary, and now the seized devices must be taken to the lab, where there is a permanent isolation solution [14]. We are also required to keep the devices charged to prevent a lockdown [14].

2.2 The Forensic Analysis Process

When the devices arrive at the lab, we place them in permanent isolation. It can range from a little shielded container to an entire room [14]. The latter is preferred as it allows analysts to work freely.

We will now review the process of smartphone forensic analysis using the Harmonized Mobile Forensic Investigation Process Model [15], comprised of seven layers or phases:

1. Preparation.
2. Preservation.
3. Data Acquisition.
4. Examination.
5. Analysis.
6. Reporting.
7. Presentation.

10.11228/dpsc.03.01.008

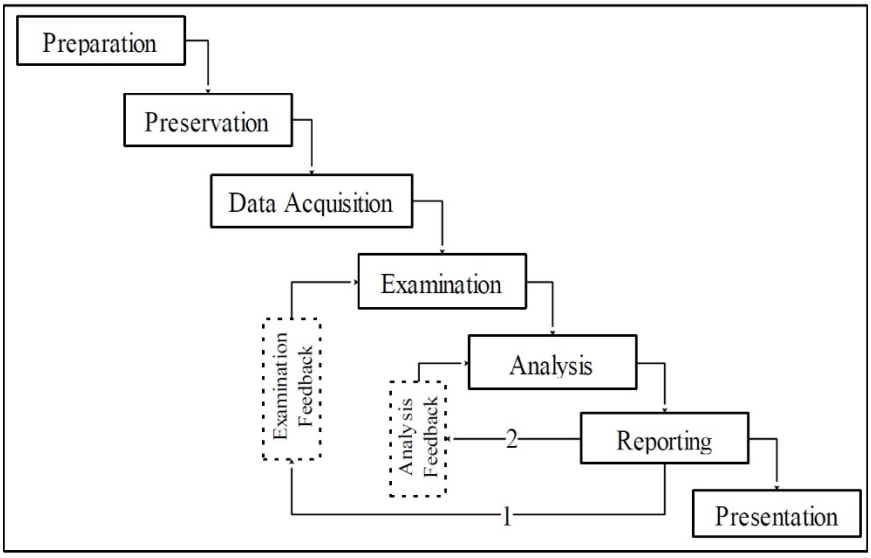


Fig. 1. Harmonized Mobile Forensic Investigation Process Model [15]

Preparation. This phase refers to creating a clean and isolated forensic environment to conduct the investigation. A clean environment is vital to guarantee that our evidence is not contaminated with evidence from another investigation, while the isolation is crucial to prevent any data loss. We also define what verified forensic techniques we will use and how the device will be isolated [1],[15].

Before we do anything to the device, we must first correctly identify it and catalog it. This way, we can avoid any mix-ups and choose which techniques and tools we use more efficiently.

Preservation. This phase refers to the process of preserving the integrity of the device and its data [15]. This phase is significant, as any tampering, be it accidentally or intentionally, can compromise the validity of the evidence on the device [1],[14].

We calculate the hashes[1] of all the files present on the device to later compare with those from extracted files, ensuring data integrity. We also take note of all the file timestamps for later comparison.

Data acquisition. This phase refers to acquiring, sometimes called extracting, the device's data, and any digital identifiers [15]. This phase is the most crucial in the whole process [14], and there are various techniques and tools available to analysts.

It is also vital to ensure a tool is compatible with the device and has a consistent output, and we do this by using it on another device of the same make and model [14]. The tool must block the operating system from updating any file timestamps or any

[1] Bit string with fixed size calculated using one-way hashing algorithms

10.11228/dpsc.03.01.008

writing operation. Otherwise, we would compromise data integrity or overwrite some crucial information, invalidating the evidence.

Examination. This phase refers to examining the acquired data to ensure its authenticity and not being tampered with in any way [15]. We compare file hashes and timestamps with the previously calculated ones to guarantee that any tampering has occurred and that file integrity remains unviolated.

Analysis. This phase refers to analyzing the examined data from the previous phase. We usually use special forensic tools to reconstruct the device's activities and recover who, when, and where these activities happened.

In modern devices running Android or iOS, this usually means sifting through many SQLite databases [14], [15]. These are the preferred method to store application data, including system ones like messages, calls, and contacts, which nowadays run on top of applications. Even though databases can have many lines, they have the advantage of providing access to deleted data sometimes.

Other file types such as images, videos, and documents may be significant for investigations and serve as direct evidence in court, but log files more often than not represent a treasure chest of past activities [4],[16]. These log files can include user authentication events, permission changes, unique identifiers generated by applications, application usage telemetry, geolocation information, network activity, deleted file names, and many other useful data. The best thing about log files is that everything has a timestamp.

The forensic tools are a huge help in sorting, filtering, and searching through all this data, sometimes even alert analysts of any interesting information.

Reporting. This phase refers to documenting or reporting all investigation steps [1],[15]. This phase has two feedback processes: the examination feedback and the analysis feedback [15].

In the examination feedback, we re-integrate and re-evaluate the information to revise any discrepancies or update the examination process [15]. In the analysis feedback, we re-analyze the information outputted from the examination feedback [15].

If we find any discrepancy in any of these feedback processes, we must repeat the process chain from the point we returned to [15], as shown in the flowchart represented in figure 1.

Presentation. This phase refers to the process of presenting our findings to law enforcement. As previously stated, these findings can be used as evidence in a court of law or to help in an ongoing investigation [1],[15]. This phase is the final one in a forensic investigation.

10.11228/dpsc.03.01.008

2.3 Data Acquisition Techniques and Tools

The data acquisition phase is the most critical part of the forensic analysis process [14]. We will examine what techniques are available to analysts and what tools they can use in each one.

The first technique is the simplest one, but it is usually only used when there is a need to access any stored information immediately. It is called manual acquisition, and this technique involves physically interacting with the device like in a standard operation scenario [17],[18].

The second one is called logical acquisition, a technique that involves making a bit-by-bit copy of the device's logical stored objects [17]. This technique is also the most used when performing forensic investigations, but it has some limitations [18]. Unfortunately, we cannot access deleted data, bypass security locks, or recover any information from damaged devices [18]. As for the tools available to conduct a logical acquisition, there are many options, but we will give only a few examples, as other products in the market do the same thing:

- ADB[2] – This tool can be used with the Android operating system and only if we can enable USB debugging on the device. Another problem is that we have limited access to the device's data, like not accessing applications that use restful encryption, meaning that the application stored data is encrypted [17].
- Backup analysis tools – There are third party tools out there capable of creating an image of the device in an external location that we can later open and analyze [17].
- AFLogical – This is a free tool available on GitHub to extract data on content providers, like SMS/MMS, call logs, contacts, or calendar [17].
- Commercial tools – There are many commercial tools by companies like Cellebrite, MOBILedit, viaForensic, MSAB, and many more [17]. Because these tools follow the same principles as the free ones, they suffer from the same caveats. The advantage of these tools is that they automate most of the process, are updated more frequently, and present the retrieved information in a much more organized manner.

The third technique at the disposal of analysts is the physical acquisition, and with it, we can make a bit-by-bit copy of the whole device, including system partitions [15]. With this technique, we can bypass security locks, recover from damaged devices, or even access deleted data since the operating system does not erase it but instead marks it as available space for overwriting [17]. As with the previous technique, this one presents a limitation, and that is the requirement to have admin or root privileges on the device [17]. For this technique, analysts can use hardware-based methods or software-based methods, in contrast to the previous technique where only software-based methods are available [17]. The methods and tools we can use for physical acquisition are:

- JTAG – This is a hardware method that relies on specifications for PCB[3] testing and debugging developed by the Joint Test Action Group. With this method, we can create images of the device's chips and retrieve their content [17].

[2] Android Debug Bridge
[3] Printed Circuit Board

10.11228/dpsc.03.01.008

- Chip-off – This is a hardware method that involves removing NAND[4] chips and resoldering them into another device, but this method can easily damage the chip's connectors [17]. This method is useful when extracting data of a damaged device or to bypass security locks [18].
- Software acquisition – There are multiple applications on the market to make a physical acquisition through software, both free and paid. However, we must root and enable USB debugging on Android devices or jailbreak iOS devices [17]. We can achieve this using exploits develop by security researchers, the same exploits people use for device customization or to run homebrew[5], and involves typically unlocking the bootloader and flashing a custom recovery or some other form of firmware exploiting [19]. The main difference between free and commercial products is that the paid solutions vendors often automate getting those admin privileges and displaying the retrieved information in a more organized manner.

3 Complications and Evolutions of the Smartphone Forensic Process

We will now talk about problems analysts face and solutions they come up with for those problems, some of which we have already mentioned in this paper. We will also be able to see the evolution of this process. Nowadays, both consumers and companies are more concerned with their privacy and security, so device manufacturers start incorporating more security measures [6]. It is important to note that these measures were implemented with security in mind, not to hinder forensic analysis purposely. The exploits used by forensic analysts are also available to hackers or any other threat actor for that matter.

The first complication worthy of mention is the implementation of security locks, as they effectively block the amount of data acquisition in most cases [17]. To overcome this problem, forensic analysts started exploiting privilege escalation vulnerabilities to perform physical acquisitions, thereby making a full copy of the device's memory and, consequently, bypassing the security lock [18].

In response to the bypasses mentioned above, some developers started making their security locks and encrypting the applications' stored data. However, as seen in recent news regarding Signal, forensic software vendors can sometimes bypass the encryption [20]. If this is possible, it can be because of poor coding of the encryption algorithm or improper storage of encryption keys, leading to possible brute-force attacks or key extraction.

To prevent privilege escalation by modifying the device's firmware, manufacturers started 006Cocking down partitions and making the user environment less permissive. One security measure was to lock the bootloader[6], preventing the overwriting of system

[4] Nonvolatile flash memory

[5] Software produced by hobbyists and amateur developers targeting proprietary hardware platforms

[6] Bootloader is a piece of code that runs before any operating system is running

10.11228/dpsc.03.01.008

partitions [21]. We must exploit the bootloader somehow to be unlocked [19], as the normal unlock procedure, even with an unlock code provided by the manufacturer, usually erases the device. After the bootloader is unlocked, it is required to flash a custom recovery, only after we can proceed with the physical acquisition [17]. Furthermore, it is worth mentioning that recently it was disclosed an iOS vulnerability at the hardware level, the now-famous checkm8 exploit [22]. A vulnerability of this severity means that any device with this specific hardware configuration and chip firmware can be exploited and is impossible to patch.

Following the same line of thought of application developers, device manufactures started implementing full disk encryption [8] or file-based encryption [7]. The use of encryption complicates things, even when using a physical acquisition technique, requiring further brute-forcing of the encryption keys.

As described in the section about device seizure, we can prevent security locks and device encryption if we seize them in an on-state [1]. By capturing a device while the user is using it, w can prevent it from being locked, and because it is operating normally, the data is currently unencrypted. Now that the device is in the authorities' hands, it is essential to keep it isolated from any network [1], and the battery charged [14].

The last complication we will talk about is anti-forensic countermeasures. To prevent any data from being overwritten or remotely erased, it is crucial to implement isolation measures on the seized devices [1] and to ensure that the battery never dies [14], basically the same solution described in the paragraph above and in the device seizure section.

4 Conclusion

In conclusion, we can see that smartphone forensics is a robust and well-defined process, but as with everything in science, still lacking some improvement and optimization. We learned how we conduct this process and how it has evolved, clearly seeing how increasingly complex it became for analysts. We also learned what complications we can encounter when performing a forensic investigation and what strategies analysts have created to overcome them, even though some problems still have no answer.

In summation, as with everything in the field of cybersecurity, smartphone forensics is a never-ending cat and mouse game. When someone discovers a new exploit, the manufacturer quickly comes up with a solution to prevent that exploit. It is up to the perfect coordination between law enforcement and forensic analysts to create new strategies and tools to solve these problems and keep the cyber world safe while not undermining everyday users' privacy.

References

1. Ayers, R., Jansen, W., Brothers, S.: Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1). NIST Spec. Publ. 1, 85 (2014).
2. How Many People Have Smartphones Worldwide (Nov 2020), https://www.bankmycell.com/blog/how-many-phones-are-in-the-world, last accessed 2020/11/09.

10.11228/dpsc.03.01.008

3. Brunty, J.: Mobile device forensics: Threats, challenges, and future trends. In: Digital Forensics: Threatscape and Best Practices. pp. 69–84. Elsevier (2016).
4. Sharma, P., Arora, D., Sakthivel, T.: Enhanced Forensic Process for Improving Mobile Cloud Traceability in Cloud-Based Mobile Applications. In: Procedia Computer Science. pp. 907–917. Elsevier B.V. (2020).
5. Ahmed, R., Dharaskar, R. V: Mobile Forensics : an Overview , Tools , Future trends and Challenges from Law Enforcement perspective. Online. 312–323 (2008).
6. Chernyshev, M., Zeadally, S., Baig, Z., Woodward, A.: Mobile Forensics: Advances, Challenges, and Research Opportunities. IEEE Secur. Priv. 15, 42–51 (2017).
7. File-Based Encryption | Android Open Source Project, https://source.android.com/security/encryption/file-based, last accessed 2020/11/11.
8. Encryption | Android Open Source Project, https://source.android.com/security/encryption, last accessed 2020/11/11.
9. Product Partitions | Android Open Source Project, https://source.android.com/devices/bootloader/partitions/product-partitions, last accessed 2020/11/14.
10. Google is rolling out end-to-end encryption for RCS in Android Messages beta - The Verge, https://www.theverge.com/2020/11/19/21574451/android-rcs-encryption-message-end-to-end-beta, last accessed 2020/11/20.
11. Signal becomes European Commission's messaging app of choice in security clampdown - The Verge, https://www.theverge.com/2020/2/24/21150918/european-commission-signal-encrypted-messaging, last accessed 2020/11/11.
12. Zoom Finally Has End-to-End Encryption. Here's How to Use It | WIRED, https://www.wired.com/story/how-to-enable-zoom-encryption/, last accessed 2020/11/18.
13. Manendra Sai, D., G K Prasad, N.R., Dekka, S.: The Forensic Process Analysis of Mobile Device. Int. J. Comput. Sci. Inf. Technol. 6, 4847–4850 (2015).
14. Raghav, S., Saxena, A.K.: Mobile forensics: Guidelines and challenges in data preservation and acquisition. In: SCOReD2009 - Proceedings of 2009 IEEE Student Conference on Research and Development. pp. 5–8 (2009).
15. Al-Dhaqm, A., Razak, S.A., Ikuesan, R.A., Kebande, V.R., Siddique, K.: A Review of Mobile Forensic Investigation Process Models. IEEE Access. 8, 173359–173375 (2020).
16. Sathe, S.C., Dongre, N.M.: Data acquisition techniques in mobile forensics. Proc. 2nd Int. Conf. Inven. Syst. Control. ICISC 2018. 280–286 (2018).
17. Alghafli, K.A., Jones, A., Martin, T.A.: Forensics data acquisition methods for mobile phones. 2012 Int. Conf. Internet Technol. Secur. Trans. ICITST 2012. 265–269 (2012).
18. Do, Q., Martini, B., Choo, K.K.R.: A cloud-focused mobile forensics methodology. IEEE Cloud Comput. 2, 60–65 (2015).
19. Signal App Crypto Cracked, Claims Cellebrite - Security Boulevard, https://securityboulevard.com/2020/12/signal-app-crypto-cracked-claims-cellebrite/, last accessed 2020/12/19.
20. Locking/Unlocking the Bootloader | Android Open Source Project, https://source.android.com/devices/bootloader/locking_unlocking, last accessed 2020/12/19.
21. Yu, M., Zhuge, J., Cao, M., Shi, Z., Jiang, L.: A survey of security vulnerability analysis, discovery, detection, and mitigation on IoT devices. Futur. Internet. 12, 1–23 (2020).

10.11228/dpsc.03.01.008

Healthcare Security and Protection in Electronic Patients' Consent: Information System SONHO case

Fernando Daniel Rocha Castro

Lusofona University of Porto, Portugal
fernandodrcastro@gmail.com

Abstract. Cybersecurity is the practice of protecting computers, networks, programs and electronic information there is against intruders or any type of virus. It also consists of recovering and fast action after an attack to avoid additional loss of information. In the medical area, all citizens that have healthcare have their personal information yielded to the hospital. Many patients don't know how they process this data and who can access it and what type of exposure they will have with a security breach.

The study of the information systems in the healthcare has the objective of understanding how electronic data of the patients are treated, used and how often the security of the systems are updated, also if the patients give the permission to use their information with another goal then what they know. To achieve this objective will be analyzed a hospital's computer system, through the research of information about this subject. System failures and possible solutions will also be presented.

Keywords: Cybersecurity, Hospital, Information, Patients, SONHO

1 Introduction

Nowadays, it is almost impossible to live without some kind of technology, which is used daily. As for health services, they have begun to evolve and adopt new technologies to make their work more practical and efficient, eliminating various problems associated with old methods (e.g., paper). However, the ease of access to some type of technology and the possibility of connecting with other devices in a network has brought several advantages, such as greater ease of obtaining, storing and sharing information, but it has also brought disadvantages, such as cybercrime attacks.

10.11228/dpsc.03.01.009

To protect a network or system it is essential to know the threats and attack techniques used by the attackers, to then implement the measures and tools needed to protect these resources. Information security is the protection of the integrity and privacy of data in databases and when they are in transit over networks. In order to use digital media in the best way and in security, it is necessary to develop and ensure their security. Digital security can be summarised in three principles [1]:

- Confidentiality of data, i.e. information is only accessed by those authorised to do so.
- Integrity, data cannot be modified and altered in an unforeseen way and the truthfulness of the information is guaranteed.
- Availability, access to information must be available to those authorised and accessible whenever requested.

Due to the little knowledge by health care users about how their personal data are treated, this work aims to understand how the information and security of health care systems in Portugal are handled. To this end, this work is composed of an analysis of security and data protection in health care facilities, as well as the Integrated Hospital Information System (Sistema Integrado de Informação Hospitalar - SONHO), which is one of the most widely used hospital information systems by the National Health System (Sistema Nacional de Saúde - SNS) in Portugal.

In addition to the present introduction section 1, the work will have 6 further sections, divided as follows:

Section 2 - discusses the concept of "Cybersecurity" and its relationship with the health institutions, reflecting on cybercrime and the ways it is celebrated in these institutions.

Section 3 - focuses on information systems and their security, emphasizing the importance of authentication, access control, standards and auditing and patient consent.

Section 4 - presents the SONHO and SONHO V2 system, its features and functionalities.

Section 5 - then identifies problems related to the SONHO system, as well as proposals for its improvement.

Section 6 - is composed of the conclusions and reflections obtained after the work was carried out.

Section 7 - presents all the references used and consulted for the present work.

2 Cybersecurity

Cybersecurity is concerned with protecting computer networks and the information they contain from accidental or malicious penetration and disruption. There is a growing concern that health information security is not sufficient, and this has already resulted in the lack of confidentiality of medical information and data integrity [2]. The Academy of Shared Services of the Ministry of Health (Serviços Partilhados do Ministério de Saúde - SPMS) with the help of the Coimbra Hospital and University

Centre (Centro hospitalar e Universitário de Coimbra - CHUC) initiated a protocol for the creation of the Centre for Development and Training in Cyber-security in Health. This is intended as an important basis for research on the safety of clinical devices, both in software and hardware. It is expected to contribute to the dissemination of all cybersecurity trials with the NHS, cybersecurity best practices, promote knowledge and training of health professionals on cybersecurity and innovation and development of cybersecurity in relation to risks to health systems. Thus, SPMS and the CHUC will establish a cooperation network, with the aim of improving the qualification of health professionals integrated in the NHS and increasing the competitiveness of the services provided [3].

2.1 CyberCrime

Cybercrime attacks range from identity data theft to more serious threats to health infrastructure and even patient security, so these attacks do much more than steal data, even hindering the daily operations of hospitals [4]. Cybercrime against health issues has manifested itself in four specific threats: data loss, theft of money, attacks on medical devices and attacks on health infrastructure. Many of these criminals are motivated by financial issues, hacking, obtaining intellectual property or consumer information to damage the institution's reputation [5]. So the best way to protect ourselves from cyber-attacks is to invest and work on the security services of healthcare institutions with robust security architectures.

Cyber-attacks, in the hospital context, can occur from several vectors [6]: 1) Internet access, if there is an Internet connection; 2) wireless network, if active wireless medical devices are used; 3) internal threat; 4) direct access attack, through physical access to a medical device; 5) removable slides such as USB, CD, PEN; 6) E-mail (e.g., phishing, Trojans); 7) other networks, access to medical slides through connection to corporate network; 8) installation or improper use, as deliberate or inadvertent activity.

3 Information System

After defining the requirements and what the institution's system should do, a number of security steps need to be taken to ensure a smooth functioning and prevent threats in the future.

3.1 Authentication

Authentication serves to identify the user and restrict access to his/her information by unauthorised persons. It is the first step in accessing the system. Authentication is essential to promote and strengthen the security of information systems. It refers to the successful identification, by some means and in some system, of a user and certifying this same identification, i.e. the system, in a controlled way, proves that the user

is who he says he is [7,8]. In most cases, the identity is proven by a cryptographic entity using a user password, which should only be known by the user. For this purpose, the security of a hospital information system is mainly based on cryptography and its authentication [9]. Thus, the computational complexity of using cryptography is used to ensure the security of all stored information is very large [9].

3.2 Access control

Another process to prevent unauthorised third-party access is to establish an access control policy. It consists of a logical entity that identifies the user who is trying to access a certain resource in the system and whether or not to allow access based on its attributes in the system. This point is central to health care information systems in order to prevent access to privileged and private information for users.

3.3 Standards and Auditing

An audit consists of a thorough analysis of the functioning of a company or organisation, assessing performance and identifying possible shortcomings that compromise its operation. In information systems, the audit goes beyond the computer function, focusing on all the information systems that belong to the organisation, whether they are computerised or not. In this way, the audit focuses on the analysis and evaluation of planning processes, developments, tests and system applications, and also examines the logical, physical, environmental, organisational, data protection and security structure [10].

ISO 27000 is a code of practice for information security and also provides security for human resources [11]. This standard address information security vocabulary and is where the ISO 270001 standard is inserted. The ISO 270001 standard is the international reference standard for Security and Information management. This standard aims to address information security management and has been improved over the years. In this way, the adoption of the ISO 27001 standard leads organisations to adopt an appropriate model for establishing, implementing, operating, monitoring, reviewing and managing an Information Security Management System, with the aim of appeasing and adequately managing the organisation's risk. Some organisations therefore require their suppliers to hold ISO 27001 certifications, as a guarantee of compliance with the principles established by ISO 27001, providing security for their customers and partners [12].

3.4 Patient consent

When a patient enters the hospital, an electronic clinical record is made, which will contain their personal data as well as data on their health status. This information can be changed and visualised by health care providers such as doctors and nurses. Clinical information systems can, for example, assist in health care delivery, clinical decision making and assess the quality of care provided. It also helps in health care man-

agement and planning. It is important to emphasise that patients have power over their access data, and thus need to give permission to access, and that they need to give their consent to those who are allowed and entitled to access that information. Patients can access their data, and health professionals, in order to securely accept patients' medical records, must use their professional identification card, and must have the patients' consent [7].

4 SONHO System

4.1 Concept

In health care in Portugal, a system was needed to store patient data and manage the financial accounting of income during their stay in hospital. To meet this need, a software was uniformly adopted in 1994 to manage the administrative data of patients, this system is called Integrated Hospital Information System (SONHO) [13], and the Central Administration of Health System (ACSS) is the institution responsible for it [14]. SONHO is the dominant information system in public hospitals in Portugal, as it has been used in a major part of SNS institutions over these years. This system is now responsible for the production control, invoicing and management of administrative data that includes clinical data such as clinical history, diagnosis and benefits. It should be noted that it is possible to export the system information for statistical indicators and to share clinical information between hospitals or even with health centres, provided they use the same information system [15]. However, in a gradual manner, SONHO is being replaced by SONHO V2, this version being more up to date according to current needs [16]. Thus, the SONHO V2 is being created as an updated and improved form of the SONHO, in order to respond to technical problems experienced by hospital units and to improve the quality and accessibility of users, health care and the improvement of working conditions for health professionals [17]. The System is connected to RIS (Rede Informática de Saúde – Health Informatics Network), a private network that interconnects several public health institutions to allow the exchange of information and services between them.

4.2 How it works

According to Pedro, V. [18], a hospital information system is developed to support administrative and clinical management with the aim of improving the equity of care provided to the user. SONHO consists of 8 modules: integrator, emergency, outpatient, inpatient, operating theatre, day hospital, archive and billing. This system incorporates three main functionalities: 1) Clinical register; 2) International classification of the patient; 3) Homogenic Diagnostic Group. At a structural level, its main objective is to create the minimum infrastructure to encompass new modules/applications interconnected with existing ones and also to ensure that the implemented standardisation criteria are naturally taken over by the new applications. On a functional level, this system focuses on controlling the flow of hospital patients. All data is collected at

hospital care points when the user accesses the entity for any type of medical act (e.g. emergency, examination) [14].

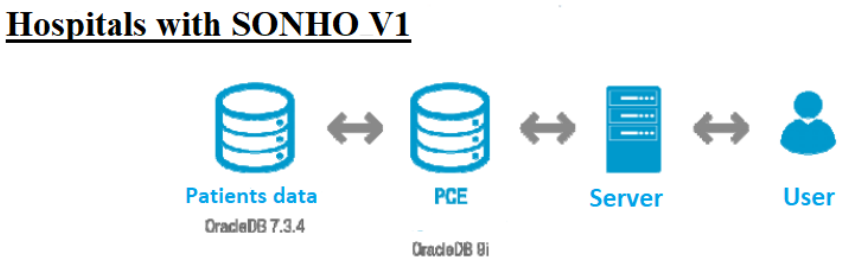


Fig. 1. Example physical architecture SONHO + PCE [16]

The first version of the SONHO revealed some difficulties in its handling, the SONHO V2 was created with the aim of combating these limitations and expanding its functionalities. The new version of SONHO V2 presents several improvements and functionalities compared to the previous version, namely [19]: a) Online help, which is a help tool that allows the user to have support in using the system; b)Upload / Download documentation, which makes it unnecessary to archive paper documentation and allows better administrative management; c) The creation of reminders for treatment, which ultimately improves the care process, d) The access to global information of each user, and the search for it quickly, e) Management of Moderator Fees, which allows access to information on the payment of moderator fees of each user; f) Use of the citizen card, which allows the identification of the user more quickly; g) Generation of Daily Maps and Statistics, h) Simultaneous scheduling of appointments, examinations and analysis; i) Consultation of several agendas simultaneously (consultations, exams and analyses); j) Visualization of a calendar with the vacancies for appointments and appointments made; k) Colour coding to identify the situation of the interned user.

4.3 LIGHT middleware

Middleware is software that is placed between an operating system and the applications that run on it. Functioning essentially as a hidden translation layer for information, middleware enables communication and data management for distributed applications. The SNS uses LIGHT (Local Interoperability Gateway for Healthcare) to mediate the exchange of information between SPMS products and external customers. It is a solution that goes beyond integration: it is an open source interoperability platform that addresses the 4 layers - legal, organisational, semantic and technical - rewarded and developed for SONHO [20]

10.11228/dpsc.03.01.009

Fig. 2. LIGHT platform [20]

5 Proposals for improvement and safety for the SONHO system

5.1 Problems

As the SONHO V1 System is old, it encounters several problems:

- maintenance level as each hospital has its own autonomous system and is checked one by one.
- It uses the same interface from the day of its creation, little oriented to the medical activity
- Poor ability to communicate with other systems which compromises the exchange of information with other health establishments using another system.
- Allows for the creation of WEB shortcuts which may compromise patient data

The personal data of the patients in the hospital information system are a fundamental and most important part, and all this information is stored in its database. As the SONHO system is an information system, it is more prone to computer attacks of the disclosure type that have the objective of stealing information. Disclosure is the unauthorised access to the information contained in the systems, and this can be divided into three types: 1) exposure, where a user or software discloses personal data to unauthorised persons; 2) interception, where a device connected to the same network can create a copy of the data when it is sent, or else have access to data transfer

10.11228/dpsc.03.01.009

traffic and intercept the information (eavesdropping); and finally, 3) intrusion, i.e. obtaining the data while ignoring the access protections to the system.

5.2 Possible solutions

To make the SONHO system more secure an authentication system could be implemented so that only authorized persons can access it. One method would be through a username and password with different access to the system depending on the status of the user in the healthcare entity.

Carrying out regular audits, this practice aims to evaluate the performance of the system and propose improvements to it, as well as possible security flaws and how to avoid them.

Protect the hardware from any possible intruder, for example by using a dedicated server room with current surveillance.

Verify the usability of the system with questionnaires to health workers using the system, with your help it is possible to orient its interface to be more interactive and easier to use, making it even more efficient. Despite all the aspects mentioned as positive in relation to SONHO V2, there are aspects that could be interesting to consider in order to further enrich and improve this new hospital information system. SONHO V2 has developed a colour coding system that allows access to the situation of hospitalized patients, however, in order to make this system more inclusive, it is important to develop other identification methods, such as the use of symbols, as there may be colour blind users with difficulties in identifying colours. Another aspect to be improved is the impossibility to digitise documents, which would be quite relevant as this would not require reference documents to be made available in several services.

Another improvement would be to integrate the Light middleware into all SNS information systems, since during the month of January 2017, around 1,932,619 events passed through LIGHT, with 97.82% of success cases [20].

6 Conclusion

The evolution of technologies and their great impact, influence and importance in information has become indispensable for many organizations and services provided today. However, the ease with which everyone can access the Internet has increased the number of hackers trying to obtain private information by illegal means, often for money. Since the beginning of the year, more than thirty public bodies have been targeted by hackers [21]. As a result, healthcare establishments that have personal data on their users in information systems databases may be the target of computer attacks from someone trying to obtain this information.

In order to prevent this loss or theft of information, it is necessary to be vigilant and carry out risk analyses periodically in order to keep up with the best solutions and improve the security of the systems. In this paper, I have explained how the SONHO, an information system used by SNS, is used to help hospitals in their administrative

part as well as to make clinical records of patients. Is also made up of a billing part that includes the costs of patients during their passage in the clinical establishment. I have presented some of its features and flaws, as well as possible improvements to make it more efficient and interactive for users, such as the use of symbols in addition to colours in the identification of patients in order to facilitate the visualisation of these for people with colorblind vision. I have had the opportunity to research and learn how healthcare institutions store their patients' information and share it among other facilities, for example, the RIS network. This has been a very important work, as it allows to know and explore a hospital information system, to identify its possible problems and to develop solutions to them, as well as to highlight the importance of personal data and the care that should be taken with them.

7 References

1. Cunha, D., & Fenato, M.: A Segurança da Informação e a sua importância para a Auditoria de Sistemas (2013)
2. Coventry, L., & Branley, D.: Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas, pp.48-52 (2018)
3. Academia SPMS: Protocolo de Cooperação em Cibersegurança na Saúde. https://academia.spms.min-saude.pt/notice/chuc/, last accessed 2020/12/15
4. Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., ... & Flahault, A.: Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making, pp.1-10 (2020)
5. Perakslis, E. D.: Cybersecurity in health care, pp.395-397 (2014)
6. Ayala: Cybersecurity for hospitals and healthcare facilities (2016)
7. Araújo, S. C.: Segurança na circulação de informação clínica. [Master's dissertation, Faculdade de Engenharia do Porto] (2007)
8. Figueiredo, D. S., Pizzol, L. C. D., & Junior, A. F. F. B.: Infraestrutura de segurança para comunicação, autenticação e autorização transparentes em hospitais federados, pp.58-63 (2011)
9. Kuang, L. Q., Zhang, Y., & Han, X.: Watermarking image authentication in hospital information system, pp.1-4 (2009)
10. Silva, P. M. G. D.: A função auditoria de sistemas de informação: modelo funcional e de competências [Doctoral dissertation, Universidade do Minho] (2008)
11. Sansigolo: A importância da série ISO 27000. Faculdade de Tecnologia de São José dos Campos (2015)
12. ISO 27001, https://www.27001.pt/index.html, last accessed 2020/12/15
13. Lameirão, S.: Gestão Hospitalar e o uso dos Sistemas de Informação: Aplicação ao CHVR-PR [Master's dissertation, Universidade de Trás-os-Montes e Alto Douro] (2007)
14. Diretório de Informação em Saúde: Sistema Integrado de Informação Hospitalar (SONHO), http://dis.dgs.pt/2010/09/30/sistema-integrado-de-informacao-hospitalar-sonho/, last accessed 2020/12/16
15. Ávila, C. I. M. D. J.: Interface para a exportação de sumários de utentes do SONHO em openEHR (2011)

16. SPMS: SPMS - Serviços Partilhados do Ministério da Saúde, www.spms.min-saude.pt, last accessed 2020/12/16
17. CHSJ Portal: SONHO V2. https://portal-chsj.min-saude.pt/pages/865, last accessed 2020/12/17
18. Pedro, V.: Adaptação do sistema de gestão de doentes do Centro Hospitalar de Leiria ao sistema integrado de gestão hospitalar SONHO V2 [Doctoral dissertation, Instituto Politécnico de Leiria] (2015)
19. Marto, V. M. A.: A Gestão da mudança em sistemas de Informação: a migração do sistema de gestão de doentes para aplicação SONHO V2 no Centro Hospitalar de Leiria, EPE V2 [Doctoral dissertation, Instituto Politécnico de Leiria] (2017)
20. SPMS: SPMS - Serviços Partilhados do Ministério da Saúde, https://www.spms.min-saude.pt/2017/02/um-ano-luz/, last accessed 2021/01/15
21. JN: Hackers sequestraram mais de 30 organismos públicos só neste ano. https://www.jn.pt/justica/hackers-sequestraram-mais-de-30-organismos-publicos-so-neste-ano-11431269.html, last accessed 2020/12/17

10.11228/dpsc.03.01.009

Review of Serious Games for Cybersecurity and Privacy Skills Training

Wendel da Silva Guimarães

Lusófona University, Porto – Portugal
weguimaraess@gmail.com

Abstract. Cybersecurity is nowadays required by any company or service, anywhere in the world. Every day this sector has a high investment in order to improve its technology and the techniques applied to it, in that same context several companies pay services and professionals that offer guarantees to maintain the security of your business and thus avoid any breach for an attack, besides to offer training to various professionals in all areas in order to avoid possible threats or vulnerabilities in the daily use of computer equipment, from simple e-mails to access to confidential information.

Similar to the growth of this area, there is a growth in the sector of serious games, these with varied purposes, in the case of this paper, we will deal here with serious games aimed at developing skills related to cyber security and privacy, where they will have a fundamental role in the professional development of the user. Currently, serious games are seen and used as tools for the development and correction of behaviors that can compromise the security of a system and help to correct them.

This paper aims to investigate how effective the use of serious games can be for training from ordinary users as well as even cyber security professionals, thus being able to portray the positive points and analyze the changes generated after their use.

Keywords: Games, Serious Games, Training, Security, Privacy

1 Introduction

As soon as we talk about cybersecurity the first thing that crosses our minds are the different types of viruses, types of attacks, information leaks and other aspects related to this, most of them linked to more serious matters. When we talk about games, we have a contrast, we associate the term with aspects related to leisure, fun, entertainment, all in a more pleasant and fun tone. However, unlike the tone addressed for games in general, we also adopt a more serious tone when we talk about the serious games theme, a theme that will be addressed in this article. Serious games are games that focus on a specific goal and not only on entertainment, these games seek to pass a different experience to the user and are mostly intended for purposes such as training, education, developing a skill, etc. At the moment there are already several sectors that make use of serious games for the purpose of learning, thus, games are used as tools for

assimilation of concepts and developments in general. It is common to see some of these sectors use serious games as a fundamental part of training, examples of which are training of students in the field of medicine that use simulation as a way to apply the concepts studied, develop decision skills among other factors. One of the areas that also make use of serious games is Cybersecurity, mostly applied with the purpose of training professionals, workers, students or even ordinary users. According to [1] "20% of the organizations who took part in the survey are using games or simulations as part of their learning solutions".

Next in the paper we will see the following topics:

- Serious games and their importance
- A brief review about cybersecurity
- The context of serious games within the cybersecurity environment
- The development of privacy skills through serious games
- Conclusion

2 Serious games and their importance

We already know that serious games are used as tools to give your player a "serious" content, which can aim at a form of training or development, however, this does not remove the fact that it is still a game, even with "serious" content being played, the game itself can be fun. They are formatted with game elements, there may be scenarios, characters and other aspects commonly seen in entertainment games, the difference here is the fact that the whole game is developed with a learning purpose, the whole focus of what is developed and presented within that game it was done with the same purpose towards the player and he must be able to convey his message. According to [2] "Playing can be part of the learning process because the subject to be learned is, at least in some respects, essentially playful. The use of serious games in the learning process therefore illuminates the fundamental nature of the subject being taught ".

Games have been used for educational purposes at least since the 20th century, they became popular in classrooms in the 60s and 70s, however, the term "serious games" only came to be used decades ahead, where the term was applied to electronic games that passed some form of learning. These games became subjects of study for some years and when they realized the advantages they brought, they started to use games with learning purposes in different sectors.

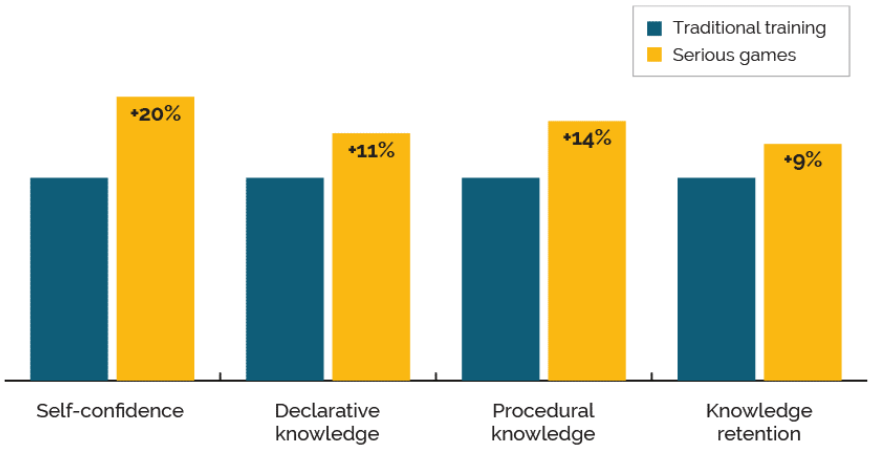


Fig. 1. Statistics about serious games (SymVision Education)

3 A brief review about cybersecurity

Given the current scenario where cybercrime is becoming more and more "common" and the forms of attack are developed in order to be more effective, the tendency is that these attacks do not stop, and with all companies and organizations being their potential targets it is necessary there are methods and policies to be adopted that can prevent these attacks from existing.

As a way of responding to these cyberattacks cybersecurity arose, acting as an active defense practice that works to avoid possible risks existing in the system and network environments, there are several ways to adopt cybersecurity, be it via antivirus software, and other tools or via hardware with firewall protections and equipment. Cybersecurity practices aim to protect against malicious attacks, avoid possible vulnerabilities and so on. It is important to note that, over the years, new forms of attacks emerge, so cybersecurity cannot be left behind and must always have its defense practices, software and hardware updated in order to try to prevent and prevent these attacks.

With all this, the cybersecurity sector is a "new" sector in the market, however there is already a large investment on the part of companies, considering that it is something essential today. According to [3] "the industry's overall growth is expected to be 12% a year through 2024, going from $ 120 billion a year in 2017 to more than $ 300 billion."

And not only software and hardware make up the cybersecurity sector, this is also an "educational" sector, to consider what as [4] said "The biggest threat is within

organizations", referring that the company's users can adopt practices that leave the system vulnerable.

In research released by [5] "Investing in employee security training and awareness can significantly reduce security-related risks from anywhere between 45 and 70 percent" and "there is an 80 percent chance that organizations with $ 200 million in annual revenue will have to pay up to $ 2.5 million a year due to insecure employee behavior. There is a 20 percent likelihood the costs from inappropriate employee behavior surpass $ 8 million ".

3.1 Internet use around the world and cybercrimes

Everywhere in the world you can see the growing trend of using the internet as an essential part of everyday life, in addition to computers, today we have Smartphones, SmartTVs, tablets, among other devices that make constant use of the internet.

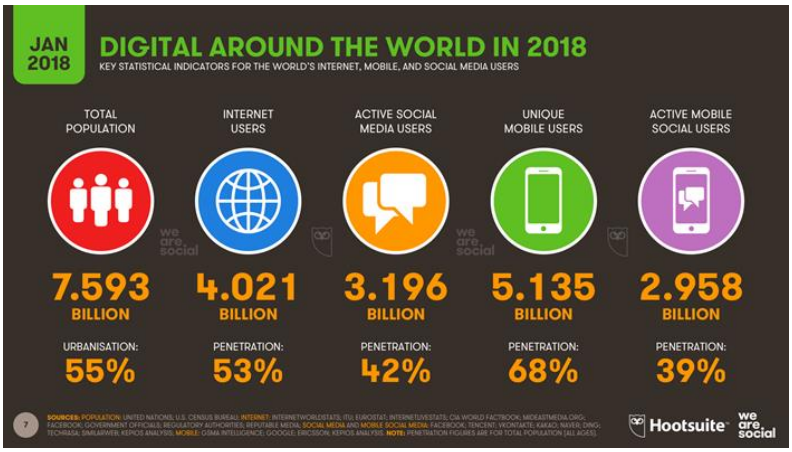


Fig. 2 Statistics about internet [6]

Together with ordinary users, companies and professionals from all over the globe use the internet in the most diverse ways for the purpose of work.

Going hand in hand with the increasing use of the internet we have cybercrime, where as the internet and its technologies advance, cybercrime develops more effective and less detectable techniques of invasion, data theft and confidential information, among other types of attacks.

The practice of cybercrime has become so common that according to [7] "about 65% of internet users have already been victims of some form of cybercrime.", When talking about cybercrime [8] said "We believe that data is the phenomenon of our time. It is

the world's new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true - even inevitable - then cybercrime, by definition, is the greatest threat to every profession, every industry, every company in the world."

With the rise of cybercrime and the growing number of attacks, according to [9] "Global Analysis organizations that suffered at least one breach in 2016 lost an average of $ 4 million."

As an example of consequences generated, we can see a famous case of a cybercrime that was reported by [10] "For a period of two years, ending in early 2015, a group of Russian-based hackers managed to gain access to secure information from more than 100 institutions around the world. The cyber criminals used malware to infiltrate banks' computer systems and gather personal data. They were then able to impersonate online bank staff to authorize fraudulent transfers, and even order ATM machines to dispense cash without a bank card. It was estimated that around £ 650 million was stolen from the financial institutions in total.

4 The context of serious games within the cybersecurity environment

Given the cybersecurity contexts, we know that this is also a training sector, with the aim of passing user policies on use, avoiding vulnerabilities, forms of defense, all to minimize the chances of a possible attack and to know how to protect themselves, and it is the from that we make use of the Serious Games.

Serious games when applied in the context of cybersecurity are used as training tools, thus having a more interactive form of learning than other more "conventional" training, these games aim to transmit a message of awareness about cybersecurity and thus pass on knowledge about the subject for these people, one of the examples of games that make use of this training mechanics involving cybersecurity is the "CyberCIEGE" of [11].

According to [12] "Development of CyberCIEGE was sponsored by the US Navy, the Naval Education and Training Command, the Office of Naval Research, the Biometrics Task Force, the Office of the Secretary of Defense, and the National Science Foundation." And about the game "CyberCIEGE enhances information assurance and cyber security education and training through the use of computer gaming techniques such as those employed in SimCity ™. In the CyberCIEGE virtual world, users spend virtual money to operate and defend their networks, and can watch the consequences of their choices, while under attack."

At the moment there are games that cover different groups of users, as both professionals and home users need to have knowledge about cybersecurity, an example of a game that can be given to both groups is the "Anti-Phishing Phil" developed by [13] and that according to [14] "Anti-Phishing Phil is an engaging online game that teaches you how to identify phishing URLs, where to look for cues in web browsers, and how to use search engines to find legitimate sites. Play for 10 minutes and learn the basics of how to spot phishing attacks. Anti-Phishing Phil is hosted by Wombat Security, and requires you to login with your CMU credentials."

There are currently several studies that portray how efficient it is to use game elements in the learning context, regardless of the age group in which the user is found, the benefits are clearly seen, thus providing positive effects and results mostly, both for the user, whether a home user or a professional, both for the company that will have an environment with safer use of its employees. You can see in the *Table 1* some examples of case studies of some games and the results they generate.

Table 1 – Papers about CyberSecurity Training Games [15]

Paper	***Game Name***	***Game Type***	***Methodology***	***Results***
[16-20]	Anti Phishing Phil	Mobile application training safety of link URLs	Think aloud, pre-test & post-test experimental vs. control, SUS usability questionnaire	Positive impact on learning, awareness and phishing susceptibility

[21-27]	CyberCIEGE	3D virtual world (sims style)	Unclear ([22]) Experiment & selfassessment ([23]) Theoretical review of cognitive principles ([24])	Sufficiently flexible to illustrate a wide range of topics and positive early indication ([23]) Positive ([24]) Unclear, but there is a need to create a science of games ([25])
[28]	"The Internet"	Unclear	Literature review	A review of elements a security network game should have
[29]	Internet Hero	Puzzle mini-games	Experiment with children	The children liked the games
[30]	PicoCTF	Web-based	Survey	Positive educational experience according to students & instructors

5 The development of privacy skills through serious games

It is commonly seen nowadays that the use of information obtained through users improves and helps to personalize their services, based on their personal tastes and in addition to making some actions more practical and simple, at first this may seem attractive to the point from the point of view of the common user, since he will mostly prefer the convenience adopted through the use of his information. On the other hand, we have a threat to the privacy of the user, where he often has no control over his own personal data or where they are used, it is possible that the user has personal data being used by third parties that not even the user had realized that he had given consent to do so.

This type of "theft" of information is based on the user's naivety and lack of knowledge about privacy, where he provides his data by himself, and these can be used in an improper way.

The term adopted for this type of action is “misuse” where it refers to the misuse of data, as defined when the data was initially collected. Often linked to the fact of inducing the user to error.

An example of misuse reported in [31] refers to “Employees at AT&T call centers in Mexico, Colombia and the Philippines were found to have stolen the names and full or partial Social Security numbers of about 280,000 of the wireless carrier's customers in the United States. The workers sold that information to third parties.”

In the same way that there are serious games to conduct cybersecurity training, there are also serious games that are used as a form of training in order to develop the user's privacy skills, they try through an interactive way to show the user the best decisions to be taken when they involve personal data or information and in addition to establish forms of safe navigation that do not compromise that same data and information.

“Some research studies show that video games encourage the acquisition of certain skills and improve student comprehension of learning materials presented through a video game”. [32]

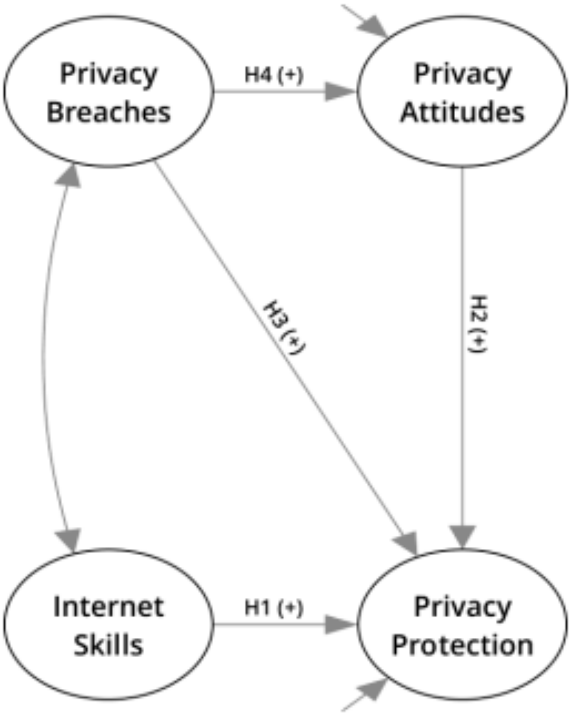


Fig. 3 Overview of the structural online privacy model [33]

The *figure 3* aims to illustrate the concept of Privacy Protection and thus demonstrate the existing structure of online privacy.

6 Conclusion

In this article we saw about serious games and their uses in the cybersecurity sectors and in the development of skills related to user privacy. Based on the research carried out, we saw that serious games can be used as interactive forms of learning and skill development, these are used as different ways of transmitting knowledge than more conventional methods. It is noteworthy that this form of learning tends to be most effective in its majority, since it is a much more active and rewarding way for those who are learning, there is satisfaction on the part of them and a desire to continue with the game, differently from watching classes, documentaries and other conventional means that are not so stimulating for those who are learning. Another advantage of serious games is that they are able to transmit diverse experiences to their "player", something that is not very possible when in training environments or classes, examples

of this are seen in simulations, mainly in the area of health in which these simulations are used to develop decision-making skills, which in real life may be able to save lives.

In the cybersecurity scenario, serious games can be used as excellent training tools, considering that most users today do not have as much knowledge about cybersecurity and no sense of the consequences and risks that this can bring, serious games are great ways to engage these same users both in the corporate and home environment, where in addition to passing on the necessary knowledge on the subject, it tries to show safe ways and security policies that can be adopted by them.

This article made me understand a little more about the cybersecurity sector and how important it is to have knowledge in order to have a safe environment. Together with that, I was also able to realize the importance of the serious gaming sector today and its effectiveness, bringing with it ways of learning and raising awareness, a form that should be more applied and distributed in different sectors, being able to transmit the knowledge of a pleasant and attractive way for more people around the globe and thus minimize the threats that reside in cyberspace.

References

1. The Towards Maturity 2012 Benchmark Report: Bridging the Gap (2012).
2. Huizinga, J.: Homo Ludens: A Study of the Play Element in Culture. Beacon Press, Boston. (1955, originally published in 1938).
3. Research Firm Global Market Insights, https://www.gminsights.com/, last accessed 2020/12/01.
4. Eben Louw, EY Senior Manager of Forensic & Integrity Services Department: Conference "Cyber Crime: from prevention to forensic response - EY" (2019).
5. Wombat Security Technologies and Aberdeen Group.: New Research From Aberdeen Group and Wombat Security Confirms Security Awareness and Training Measurably Reduces Cyber Security Risk (2015).
6. Hootsuite, used by https://www.app-scoop.com/blog/digital-transformation-why-its-important-to-your-organization, last accessed 2020/12/11 (2018).
7. NortonLifeLock Inc, https://www.nortonlifelock.com/us/en, last accessed 2020/12/01.
8. Ginni Rometty, IBM Corp.'s Chairman, President and CEO (2015).
9. Ponemon Institute's 2016 Cost of Data Breach Study (2016).
10. The New York Times: Bank Hackers Steal Millions via Malware (2015).
11. The Center for Information Systems Security Studies and Research (2014).
12. Naval Postgraduate School – US Navy, https://nps.edu/, last accessed 2020/11/15.
13. CMU Usable Privacy and Security Laboratory (CUPS), https://www.cmu.edu/iso/aware/phil/index.html, last accessed 2020/11/17.
14. Carnegie Mellon University, https://www.cmu.edu/, last accessed 2020/11/17.
15. Maurice Hendrix , Ali Al-Sherbaz and Victoria Bloom, "Game Based Cyber Security Training: are Serious Games suitable for cyber security training?", Department of Computing, School of Computing, Electronics and Maths, Coventry

University, UK and Department of Computing, School of Science and Technology, The University of Northampton, UK (2016).
16. Arachchilage G. and Asanka N., "Security awareness of computer users: A game based learning approach," Brunel University, School of Information Systems, Computing and Mathematics (2012).
17. Arachchilage N. A. G. and Love S., "A game design framework for avoiding phishing attacks," Comput. Hum. Behav., vol. 29, no. 3, pp. 706–714 (2013).
18. Arachchilage N. A. G. and Love S., "Security awareness of computer users: A phishing threat avoidance perspective," Comput. Hum. Behav., vol. 38, pp. 304–312 (2014).
19. Nyeste P. G. and Mayhorn C. B., "Training Users to Counteract Phishing," in Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 54, pp. 1956–1960 (2010).
20. Sheng S., Magnien B., Kumaraguru P., Acquisti A., Cranor L. F., Hong J., and Nunge E., "Antiphishing phil: the design and evaluation of a game that teaches people not to fall for phish," in Proceedings of the 3rd symposium on Usable privacy and security, pp. 88–99 (2007).
21. Cone B. D., Irvine C. E.,. Thompson M. F, and Nguyen T. D., "A video game for cyber security training and awareness," Comput. Secur., vol. 26, no. 1, pp. 63–72 (2007).
22. Cone B. D., Thompson M. F., C. E. Irvine, and T. D. Nguyen, Cyber Security Training and Awareness Through Game Play. Springer (2006).
23. Fung C. C., Khera V., Depickere A., Tantatsanawong P., and Boonbrahm P., "Raising information security awareness in digital ecosystem with games-a pilot study in Thailand," in Digital Ecosystems and Technologies (2008).
24. Greitze F. L., Kuchar O. A., and Huston K., "Cognitive science implications for enhancing training effectiveness in a serious gaming context," J. Educ. Resour. Comput. JERIC, vol. 7, no. 3, p. 2 (2007).
25. Irvine C. E., Thompson M. F., and Allen K., "CyberCIEGE: an information assurance teaching tool for training and awareness," DTIC Document (2005).
26. Irvine C. E. and Thompson M. F.,, "Simulation of PKI-enabled communication for identity management using CyberCIEGE," in MILITARY COMMUNICATIONS CONFERENCE, 2010-MILCOM 2010, pp. 906–911 (2010).
27. Thompson M. F and Irvine C. E., "Active Learning with the CyberCIEGE Video Game.," in CSET (2011).
28. Irvine C. E. and Thompson M., "Teaching objectives of a simulation game for computer security," DTIC Document (2003).
29. Kayali F., Wallner G., Kriglstein S., Bauer G., Martinek D., Hlavacs H., Purgathofer P., and Wölfle R., "A Case Study of a Learning Game about the Internet," in Games for Training, Education, Health and Sports, Springer, pp. 47–58 (2014).
30. Chapman P., Burket J., and Brumley D., "PicoCTF: A Game-Based Computer Security Competition for High School Students," 2014 USENIX Summit Gaming Games Gamification Secur. Educ. 3GSE 14 (2014).
31. The New York Times: F.C.C. Fines ATT $25 Million for Privacy Breach (2015).
32. Conolly, T., Stansfield, M., Boyle, L..: Games-Based Learning Advancements for Multy-Sensory Human Computer Interfaces: Techniques and Effective Practices. IGI GlobalPublishing, (2009).
33. Büchi, M., Just, N., & Latzer, M. - Caring is not enough: The importance of Internet skills for online privacy protection. Information, Communication & Society (2016).

Proceedings of the Digital Privacy and Security Conference 2021 10.11228/dpsc.03.01

Papers in alphabetical order

Authors in alphabetical order

Conference EOI :10.11228/dpsc
DPSC2021 Proceedings EOI: http://eoi.citefactor.org/10.11228/dpsc

PRIVACY AND SECURITY CONFERENCE 2021

PRIVACYANDSECURITYCONFERENCE.PT