PRIVACY AND SECURITY CONFERENCE 2020

PRIVACYANDSECURITYCONFERENCE.PT

Proceedings of the Digital Privacy and Security Conference 2020

15 January 2020 *Porto, Portugal*

Editors
Carla Cordeiro and Hugo Barbosa

UNIVERSIDADE LUSÓFONA DO PORTO

COPYRIGHT

While every precaution has been taken in preparing this book, publishers and authors assume no responsibility for errors or omissions, or for damages resulting from use of the information contained herein.

1st Edition 2020

Issue EOI:10.11228/dpsc.02.01

Editors: Carla Cordeiro and Hugo Barbosa

Proceedings Design: Hugo Barbosa

Graphical Design/Website: Hugo Barbosa

E-mail: hugo.barbosa@ulp.pt

Conference Website: http://privacyandsecurityconference.pt

Conference EOI :10.11228/dpsc
DPSC2020 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

Steering and Scientific Committees

Digital Privacy and Security Conference 2020 steering and scientific committees welcome you to the third edition of the conference. The main goal of a scientific event disseminate and create knowledge. Organizing this conference proved to be a challenging opportunity for us to achieve this goal.

Today, the digital world is transforming society at an unprecedented rate. But the growth of cyber threats, regulation and business requirements creates new challenges for success and the adoption of digital transformation programs. Our commitment and 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 motivation constitute the driving force which stimulates students of Supplementary Networking course, 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 and computer networks. The grouping of this information, which takes the shape of a proceedings 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.

Thanks to all the sponsors who made the conference possible, as well as all those who contributed to the success of DPSC2020.

Porto, January 2020
Carla Cordeiro and Hugo Barbosa

Conference Committees

STEERING COMMITTEE

Carla Moreira Cordeiro (Lusofona University of Porto, Portugal)

Hugo Azevedo Barbosa (Lusofona University of Porto, Portugal)

SCIENTIFIC COMMITTEE

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)

Nuno Santos (IST - University of Lisbon, Portugal)

Miguel Frade (CIIC/IPL - Polytechnic Institute of Leiria, Portugal)

João Ulisses (University of Vigo, Spain)

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

Esma Aïmeur (University of Montreal, Canada)

Weizhi Meng (Technical University of Denmark, Denmark)

Günther Pernul (University of Regensburg, Germany)

SUPPORT COMMITTEE

Catarina Freitas (EPCJC, Portugal)

Cíntia Torres (EPCJC, Portugal)

Maria Oliveira (EPCJC, Portugal)

CONTENTS

SESSION 1 - Cyber Threats and Security Systems

Web Applications Security Risk Quantification Based on Review of Past Six OWASP Top-10 ……...............................…………………………..…. page 8
Amjad Zareen and Mansoor Ahmed Khan

A Survey of Cyber Security Systems: Approaches for Attack Detection, Prediction and Prevention.......................…………………………..…. page 21
Jorge Gonçalves and Hugo Barbosa

A Survey of Cyber Security Systems: Approaches for Attack Detection, Prediction, and Prevention......……………………………………..…... page 33
Vera Oliveira

Review of cyber threats on Educational Institutions.............................. page 43
Jorge Pinheiro

Portugal Cyber threats Review: Targeted Health Institution...........….. page 52
David Pinto

Information Privacy and Security on a Shared Resources Network: IP Spoofing Attacks..................……………………………………..…... page 61
Pedro Graça

SESSION 2 - Digital Contents Challenges in the Era of Digital

Analysis of Security in E-Commerce and M-Commerce ..……..……. page 74
Nuno Mata

Major Challenges in Digital Contents Copyright Protection.....………. page 86
André Fontes

Major Challenges in Digital Contents Copyright Protection......……… page 96
João Barreira

A Survey of Android Attacks Detection Techniques........................... page 106
José Duarte

Android Attacks Detection Techniques...........……..……………….. page 118
Hugo Marques

SESSION 1

Cyber Threats and Security Systems

Web Applications Security Risk Quantification Based on Review of Past Six OWASP Top-10

Amjad Zareen and Mansoor Ahmed Khan

A Survey of Cyber Security Systems: Approaches for Attack Detection, Prediction and Prevention
Jorge Gonçalves and Hugo Barbosa

A Survey of Cyber Security Systems: Approaches for Attack Detection, Prediction and Prevention

Vera Oliveira

Review of cyber threats on Educational Institutions

Jorge Pinheiro

Portugal Cyber threats Review: Targeted Health Institution

David Pinto

Information Privacy and Security on a Shared Resources Network: IP Spoofing Attacks

Pedro Graça

Web Applications Security Risk Quantification Based on Review of Past Six OWASP Top-10

Amjad Zareen[1], Dr Mansoor Ahmed Khan [2]

[1]MS Info Sec, Institute of Avionics and Aeronautics
Air University Islamabad, Pakistan
amjad.zareen@yahoo.com
[2]Institute of Avionics and Aeronautics, Air University
Islamabad, Pakistan
mansoorkhan75@gmail.com

Abstract. Since year 2003, OWASP has remained prominent in cyber security paradigm by continually publishing Top-10 Web Application Security risks. In this paper, Web Application Security Risk quantification has been produced and visualized. Review of past six OWASP Top-10 has been presented in such a manner which reveals evolution and helps to induce relationshep among risks. Transformation of risks demonstrated that web applications attacks such as Injection, Cross Site Scripting (XSS) and Broken Authentication which were present about two decades ago still prevail in present day scenarios. Data visualization using Python has been demonstrated while developing a keywords finding script from any research text as part of this research.

Keywords: OWASP Top-10, Web Applications, Access, Security, Control, Injection, Risks, Vulnerablities.

1 OWASP Top-10

The Open Web Application Security Project known as OWASP is an open community dedicated to enable organizations to develop, purchase and maintain web applications that can be trusted [1]. OWASP acts as great resource for finding web application security development libraries, penetration testing tools, standards and books. OWASP is kind of organization that claims to be free from commercial pressures and provides impartial, useful and cost-effective information about web applications security. Vulnerable web applications and security issues continue to undermine various sectors in electronic industries. The goal of OWASP Top-10 project is to raise awareness about web applications security by identifying most critical risks being faced by the organizations [2]. The OWASP is referred by many security standards, books, tools and organizations. About 99% of web applications that were tested in 2012 have reveled one or more serious security

10.11228/dpsc.02.01.001

vulnerabilities [3]. On average, the number of security issues affecting each web application increased from approximately 12.5 in 2010 to 13.5 in 2011 before declining to 12.1 in 2012 [4]. Study of 2018 cyber threats reveled that; three most common attacks on websites: SQL Injection, Path Traversal and Cross-Site Scripting (XSS) have remained the same for many years [5]. Web applications vulnerability statistics of year 2018 further divulge that, on average, each web application contained 33 vulnerabilities, out of which 6 were of high severity. In 19 percent of tested web applications, vulnerabilities allow an attacker to take control of the application and server OS [5]. The number of critical vulnerabilities per web application grew by 3 times compared to 2017. With such a high number of vulnerabilities per web application, it is no wonder that, web application attacks are focal point for hackers now a day.

1.1 History and Methodology

The OWASP Top-10 was first released in 2003. OWASP 2004 Top-10 list represented the combined wisdom of OWASP experts. Then it was released again with minor updates in 2007. Till 2007, the web applications vulnerabilities were listed based on their prevalence. OWASP 2007 Top-10 methodology extracted Top-10 web application security issues based on vulnerability trends. Afterwards, OWASP risk ranking methodology devised a formula: Risk = Likelihood * Impact [6]. The OWASP 2010 version reorganized and prioritized risks not just by occurrences. Risk ranking methodology used in year 2010 included three Likelihood factors: prevalence, detectability, ease of exploit and one Impact factor: technical impact. Prevalence statistics from number of different organizations were obtained and their average data produced Top-10 likelihood list by prevalence. This was then combined with likelihood factors: detectability and ease of exploit in order to calculate likelihood rating for each weakness. The result was then multiplied by estimated average technical impact to come up with an overall risk ranking. OWASP Top-10 for 2013 marked the project's tenth anniversary and followed similar approach as of year 2010. OWASP Top-10 project felt accelerated changes over the recent past years while categorizing Top-10 for year 2017. OWASP Top-10 for year 2017 was re-factored and methodology was fully revamped. They utilized a new data call process, worked with the community, reordered risks, rewritten each risk from the ground up and added references for web applications development frameworks and commonly used programming languages and the available time to take rectification actions. The simplified description of latest web applications risks described in OWASP Top-10 and their transformation has been explained in later part of this paper.

1.2 Comparison and Relationship

The threat landscape of web applications has continually evolved during the past sixteen years with the advent of new attack techniques and technologies. Inevitably, the web applications developers need to remain cognizant of specific risks and mitigation techniques to ensure business continuity with acceptable level of cyber protection. It is not surprising that OWASP Top-10 list has evolved radically over time in terms of rankings. Based on the OWASP Top-10 review and comparison of six releases 2003, 2004, 2007, 2010, 2013 and 2017 a relationship in tabular form has been produced in a manner which can help finding evolution process among different web applications vulnerabilities with a careful glance [Table-1]. While looking at the relationship among risks and vulnerabilities presented, it can be easily recognized that the vulnerabilities and associated risks such as Injection, Cross Site Scripting (XSS) and Broken Authentication present about two decades earlier still remain prevailing in web applications.

2 Risks That Have Not Transformed

2.1 Injection

Injection attacks is one of the most damaging and high priority vulnerability across the web applications [7]. Injections attacks can result: data destruction, planting of malicious data or code and sensitive information leakage. Injection vulnerabilities such as SQL, OS or LDAP occurs when un-trusted data is sent to the interpreter as part of a legtimate command or query. The attacker's crafted data can trick the interpreter into executing unintended commands. Same can result access to unauthorized data or even destroy valuable records. Injection attacks have dominated the top of web application vulnerability lists for the past decade. Injection vulnerabilities are applicable to frequently accessing relational databases by web applications using SQL commands. Web applications usage may involve operations like searching, registration, online payments and logins etc. which can be used as source for injecting malicious input by attackers. Injection attacks can be conceded simply by using a browser, as most of the time port 80 or 443 are not blocked by firewalls for serving legitimate HTTP and HTTPS requests. Careful crafting and injection of inputs with the help of error analysis can lead the attacker to even take complete control of backend Server / Database / OS. Injection can be of different types. Command Injection type refer an attack where user becomes capable of injecting code into a command line. Unchecked File Uploads become dangerous when user is allowed to upload all kind of files including executable. Code Injection becomes possible where user can directly inject executable code of choice.

2.2 Broken Authentication and Session Management

Broken Authentication and Session management vulnerability usually occur due to non-standardized implementation of web application functions related to authentication and session management [8]. Due to this vulnerability, an application inappropriately allows attackers to exclaim themselves as valid user or an unauthenticated user can act as authorized user.

Table-1: Relationship among OWASP Top-10 past Six Releases

Rating & Risk Score	Year 2003	Year 2004	Year 2007	Year 2010	Year 2013	Year 2017
A1-100	Un-validated parameters	Un-validated Input	Cross Site Scripting (XSS)	Injection	Injection	Injection
A2-90	Broken Access Control	Broken Access Control	Injection Flaws	Cross-Site Scripting (XSS)	Broken Authentication and Session Management	Broken Authentication
A3-80	Broken Account and Session Management	Broken Authentication and Session Management	Malicious File Execution (NEW)	Broken Authentication and Session Management	Cross-Site Scripting (XSS)	Sensitive Data Exposure
A4-70	Cross Site Scripting (XSS)	Cross Site Scripting (XSS)	Insecure Direct Object Reference	Insecure Direct Object References	Insecure Direct Object References	XML External Entities (XXE)
A5-60	Buffer Overflows	Buffer Overflows	Cross Site Request Forgery -CSRF (NEW)	Cross-Site Request Forgery (CSRF)	Security Misconfiguration	Broken Access Control
A6-50	Command Injection Flaws	Injection Flaws	Information Leakage and Improper Error Handling	Security Misconfiguration	Sensitive Data Exposure	Security Misconfiguration
A7-40	Error Handling Problems	Improper Error Handling	Broken Authentication and Session Management	Insecure Cryptographic Storage	Missing Function Level Access Control	Cross-Site Scripting (XSS)
A8-30	Insecure Use of Cryptography	Insecure Storage	Insecure Cryptographic Storage	Failure to Restrict URL Access	Cross-Site Request Forgery (CSRF)	Insecure Deserialization
A9-20	Remote Administration Flaws	Denial of Service	Insecure Communications (NEW)	Insufficient Transport Layer Protection	Using Components with Known Vulnerabilities	Using Components with Known Vulnerabilities
A10-10	Web and Application Server Misconfiguration	Insecure Configuration Management	Failure to Restrict URL Access	Un-validated Redirects and Forwards (NEW)	Un-validated Redirects and Forwards	Insufficient Logging & Monitoring (NEW)

A session hijacking can also occur where a hacker takes control of a user session after successfully obtaining or generating an authentication session ID. This can be achieved by using captured, brute-force or reverse-engineering of session IDs to seize control of a legitimate user's Web application session while that session is in progress.

2.3 Cross Site Scripting (XSS)

Cross Site Scripting (XSS) vulnerability occurs whenever an application takes data that originates from a user or program and sends it to the browser without validating or properly encoding [9]. XSS allows hackers to execute scripts in the victim's browser, which can hijack user sessions, deface web site, redirect the user to malicious site or conduct phishing attacks. Cross Site Scripting (XSS) was the most frequently found vulnerability in apps tested in 2012 [3].

2.4 Cross Site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of attacker. CSRF can be as powerful as the web application that is being attacked. Cross-Site Request Forgery (CSRF) was found in only 5% of applications during year 2017, as many web development frameworks now a days include CSRF defenses [10].

2.5 Un-Validated Redirects and Forwards

Web applications frequently redirect and forward users to other web pages and websites and use un-trusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages [11].

2.6 Security Misconfiguration

Security misconfiguration is commonly found issue in OWASP Top-10. This is result of: insecure or use of default configurations, incomplete or ad-hoc configurations, open cloud storage, misconfigured HTTP headers and verbose error messages containing sensitive information [10]. All operating systems, development frameworks, libraries and web applications need secure configurations with proper error handling messages and updated security patch in order to safeguard against this risk.

3 Risks That Have Evolved

3.1 Broken Access Control

This results when restrictions on what authenticated users are allowed to do are not properly enforced [10]. Attackers can exploit these flaws to access other users' accounts, view sensitive files or use unauthorized functions. Example of such attack scenario could be; when an authenticated user of online banking while performing own transaction may get access to other user accounts. Access control also known as authorization mechanism, is how a web application grants access to content and functions to legitimate users and deny others. These checks are performed after authentication and govern what 'authorized' users are allowed to do. Access control sounds like a simple problem but is difficult to implement correctly and require due diligence and care. A web application's access control model is closely tied to the content and functions that the web application provides. In addition, the users may fall into a number of groups or roles with different abilities or privileges [12]. Developers frequently underestimate the difficulty of implementing a reliable access control. Many of access control schemes were not designed deliberately, but have evolved along with the web applications. In such cases, access control rules are inserted in various locations all over the source code. As the application reaches the deployment stage, the ad-hoc collection of rules becomes so unwieldy that it transforms almost impossible to understand. Many of such flawed access control schemes are not difficult to discover by hackers. In addition to viewing unauthorized content or performing illegitimate transactions, an attacker might be able to change or delete content, perform unauthorized functions or even take over complete web administration. In 2004 OWASP Top-10 Remote Administration Flaws merged Broken Access Control category as a special case of that category.

Remote Administration Flaws. One specific type of access control problem is administrative interfaces that allow web application administrators to manage their applications over the Internet or Intranet [13]. Such features are frequently required to manage users, data and content for the web applications. In many occasions, sites support a variety of administrative role to allow finer granularity of site administration. Due to their power, these interfaces are frequently prime targets for attack by both outsiders and insiders.

Insecure Direct Object Reference. A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as file, directory or database [14]. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data. It appeared first time in OWASP year 2007 Top-10 when Broken Access Control present in 2003 / 2004 divided into Insecure Direct Object Reference and Failure to Restrict URL Access. Insecure Direct Object Reference remained present in OWASP Top-10 for year 2010 and 2013.

Failure to Restrict URL Access. Frequently, the only protection for a URL is that links to that page are not shown to unauthorized users [15]. However, a motivated, skilled or just plain lucky attacker may be able to find and access hidden pages, invoke functions, Web Services or APIs and able to manipulate data access by crafting URLs. Security by obscurity is not sufficient to protect sensitive functions and data in an application. Access control checks must be performed before a request to a sensitive function, Web Service or APIs is granted, which ensures that the user is authorized to access that functionality. In 2013 OWASP Top-10 Failure to Restrict URL Access expanded into Missing Function Level Access Control.

Missing Function Level Access Control. Most web applications verify function level access rights before making that functionality visible in the User Interface. However, applications need to perform similar access control check on the server side when each function is accessed [14]. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization. Insecure Direct Object References and Missing Function Level Access Control from OWASP Top 10 year 2013 were merged into Broken Access Control in year 2017.

3.2 Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application / web / database server, underlying operating system and infrastructure cloud platforms [11]. Secure configuration settings needs to be defined, implemented and maintained. Additionally, firmware and software need to be kept up to date with latest and tested security patches. Security Misconfiguration appeared on 2010 OWASP Top-10 and was further divided in 2013 OWASP Top-10 into Security Misconfiguration and Using Components with Known Vulnerabilities. When Security Misconfiguration appeared in 2010 OWASP Top-10; it covered Malicious File Execution and Information Leakage / Error Handling listing of 2007 OWASP Top-10.

Information Leakage and Error Handling. Web applications can unintentionally leak information about their configuration, internal workings, structure and methods or may violate privacy through a variety of misconfigured error handling [16]. Attackers can use this weakness in order to gather information for stealing sensitive data or conducting serious attacks.

Malicious File Execution. Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, which can result in devastating attacks, such as total server compromise [17]. Malicious file execution attacks affect PHP, XML and any framework where filenames or files from users are accepted.

3.3 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs and authentication credentials such as passwords [11]. Attackers may steal or modify weakly protected data to conduct online fraud, identity theft or other cybercrimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with browsers. When Sensitive Data Exposure appeared in 2013 OWASP Top-10; it covered Insecure Cryptographic Storage and Insufficient Transport Layer Protection listings of 2010 OWASP Top-10. Insufficient Transport Layer Protection was previously named as Insecure Communications in 2007 OWASP Top-10. Insecure Cryptographic Storage of 2007 OWASP Top-10 evolved from Insecure Storage of 2004 OWASP Top-10 which itself evolved from 2003 OWASP Top-10 Insecure Use of Cryptography.

Insecure Cryptographic Storage. Many web applications do not properly protect sensitive data, such as credit cards, SSNs, and authentication credentials, with appropriate encryption or hashing [17]. Attackers may steal or modify weakly protected data to conduct identity theft, credit card fraud or other crimes. Encryption algorithms with correct implementation and assured key management are desired.

Insufficient Transport Layer Protection. Applications frequently fail to authenticate, encrypt and protect the confidentiality and integrity of sensitive network traffic while in-transit [18]. When they do, they sometimes support weak algorithms, use expired or invalid certificates, or do not implement them correctly.

Insecure Communications. Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications [18]. Man in the Middle attack protection mechanism are desirable for such scenarios.

Insecure Storage. Most web applications need to store sensitive information, either in a database or on in a file system. The information might be passwords, credit card numbers, account records or any other proprietary data [18]. Frequently, symmetric encryption techniques are used to protect sensitive information. While encryption has become relatively easy to implement and use, developers still frequently make mistakes while integrating it into a web applications. Developers may overestimate the protection gained by using encryption and not be as careful in securing other aspects.

3.4 Using Components with Known Vulnerabilities

Components, such as software libraries, frameworks, and other modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or system takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts. Security evaluation of such components is prerequisite prior to using them in a sensitive development environment.

3.5 XML External Entities (XXE)

This is a new category in OWASP Top 10 for year 2017 primarily supported by (source code analysis security testing tools (SAST) data sets. OWASP Top-10 for year 2017 asked the community to provide insight into two forward looking weakness categories. After over 500 peer submissions and removing issues that were already supported by data such as Sensitive Data Exposure and XXE, the two new issues were listed as XML External Entities (XXE) and Insecure Deserialization. Un-validated Redirects and Forwards, while found in approximately 8% of web applications, was overall edged out by XXE in OWASP Top 10 of year 2017 [10].

3.6 Insecure Deserialization

This permits remote code execution or sensitive object manipulation on affected platforms. It occurs when untrusted data is used to abuse the logic of an application, inflict a Denial of Service (DoS) attack or even execute arbitrary code upon it being deserialized. Serialization refers to a process of converting an object into a format which can be persevered to disk. Examples include: save to a file or a datastore, sent through streams or sent over a network. The format in which an object is serialized, can either be binary or structured text like XML, JSON etc. Deserialization is the opposite of serialization and involves transforming serialized data back into an object. Safe deserialization of objects must be considered as normal practice in software development [19]. The trouble can start when deserializing is done on untrusted inputs.

3.7 Insufficient Logging & Monitoring

Lack of this can significantly delay malicious activity and breach detection, incident response and digital forensics investigations. Insufficient Logging & Monitoring risk differs from other risks. While it cannot lead to a direct intrusion, existence of this results in failure to detect the intrusion in a timely manner. A failure that can cost significant in monetary as well as technical terms.

4 Risk Analysis and Quantification

Many different approaches exist for carrying out information security risk analysis for web applications. The OWASP approach is customized for web applications security and is based on simplest formula as follows:-

Risk = Likelihood * Impact [6]

The above formula has been applied for the purpose of quantification and graphical depiction on Top-3 risks which consistently remained present in Web Applications. Likelihood for a risk has been labelled numerically on scale of 10 to 100. Risk having A1 rating in OWASP Top-10 has been assigned a score of 100 while A10 rating is quantified as 10. Impact factor has been assumed constant for simplification. Most of the times, impacts such as reputation loss, financial loss, data loss etc. are truly hard to quantify in real sense. Based on the risk analysis quantification; Injection attack has been found most prevalent and ranked as most dangerous as depicted in Figure-1.

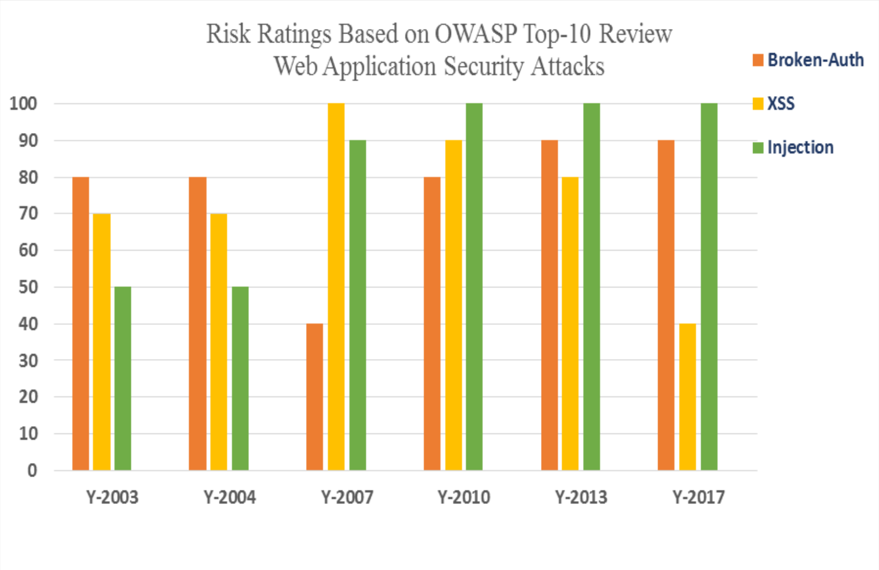


Figure 1. Risk Ratings Based on past six OWASP Top-10 Review

5 Keywords Discovery from Research

Keywords are words that capture the spirit of any research paper. Keywords make research paper searchable and ensure to attract citations. It is significant to contain the most relevant keywords that help other authors. Conference and Journal ask for varied number of keywords. Research text data parsing and its visualization using Python script has been demonstrated for finding variable number of keywords from any research text. The results obtained from this paper are appended in Figure-2.

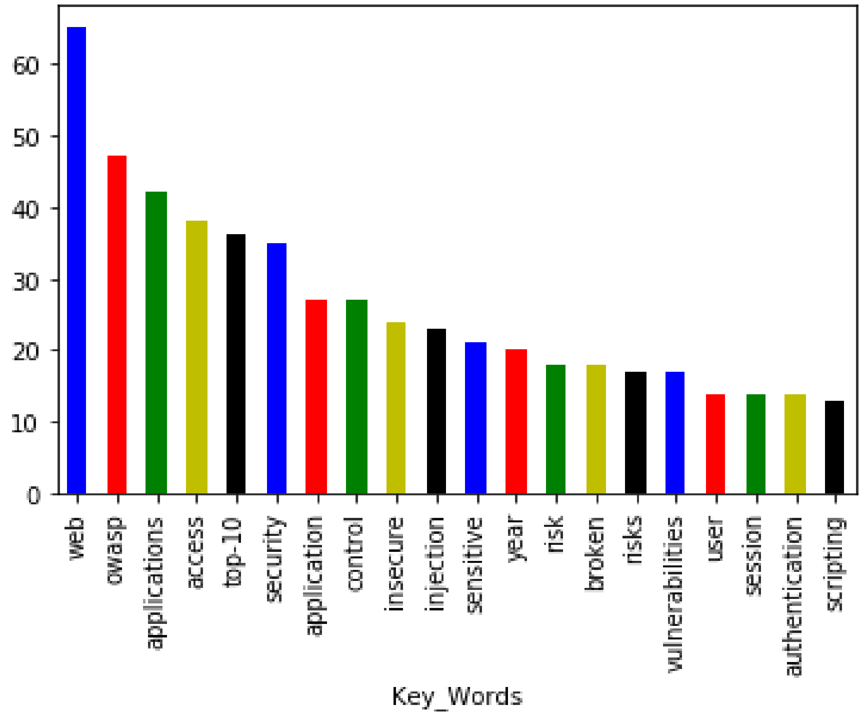


Figure 2. Research Keywords Visualization using Python

6 Conclusion

Web applications risks including Injection, Cross Site Scripting (XSS) and Broken Authentication remained consistently present in OWASP Top-10. Injection has been quantified as the top most risk based on review of past six OWASP Top-10. Modern day attackers are targeting web applications security vulnerabilities for gaining access to sensitive data. Organizations need to show vigour with greater extents to protect web applications. As more organizations are touching towards cloud transformation, web applications security is becoming more crucial. Risks and associated attacks presented in this research predominantly relate to the software development domain and demand serious attention. These problems require secure development, secure implementation and continuous monitoring practices for attaining sustainable cyber security posture. Keeping the same in view a comprehensive model comprising people, technology and processes is deemed essential to address consistently present web applications security risks.

References

1. Open Web Application Security Project – OWASP Foundation [Online] Available: https://www.owasp.org [Accessed 10 January, 2020]

2. OWASP Top-10 Project [Online] Available: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project [Accessed 11 January, 2020]

3. Application Vulnerability Trends Report : 2013 [Online] Available: http://expo-itsecurity.ru/upload/iblock/ffb/cenzic-application-vulnerability-trends-report-2013.pdf [Accessed 11 October, 2018]

4. Web Application Vulnerability Statistics 2013 by Eyal Estrin [Online] Available: http://www.contextis.com/files/Web_Application_Vulnerability_Statistics_-_June_2013.pdf [Accessed 24 December, 2018]

5. Attacks on Web Applications: 2018 in Review [Online] Available: https://www.ptsecurity.com/ww-en/analytics/web-application-vulnerabilities-statistics-2019/ [Accessed 11 January, 2020]

6. OWASP Risk Rating Methodology [Online] Available: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology [Accessed 10 January, 2020]

7. SQL Injection Attacks on Web Applications by Chandershekhar Sharma ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 3, March 2014 [Online] Available: https://www.researchgate.net/publication/320076267_SQL_Injection_Attacks_on_Web_Applications [Accessed 11 January, 2020]

8. The Importance of Broken Authentication and Session Management to Application Security by Anita D'Amico [Online] Available: https://codedx.com/blog/broken-authentication-and-session-management/ [Accessed 10 January, 2020]

9. Microsoft document for Preventing Cross-Site Scripting (XSS) By Rick Anderson [Online] Available: https://docs.microsoft.com/en-us/aspnet/core/security/cross-site-scripting [Accessed 11 January, 2020]

10. OWASP Top 10-2017 Release Notes [Online] Available: https://www.owasp.org/index.php/Top_10-2017_Release_Notes [Accessed 26 December, 2019]

11. OWASP Top 10-2013 [Online] Available:
https://www.owasp.org/index.php/Top_10_2013-Top_10
[Accessed 24 December, 2019]

12. Broken Access Control [Online] Available:
https://www.owasp.org/index.php/Broken_Access_Control
[Accessed 18 December, 2019]

13. A2 2004 Broken Access Control [Online] Available:
https://www.owasp.org/index.php/A2_2004_Broken_Access_Control
[Accessed 10 December, 2019]

14. Must Known Web Security Risks for Developers By Sanjeev Murthy
[Online] Available:
https://www.pluralsight.com/guides/must-known-web-security-risks-for-developers
[Accessed 18 November, 2019]

15. Top 10 2007-Failure to Restrict URL Access [Online] Available:
https://www.owasp.org/index.php/Top_10_2007-Failure_to_Restrict_URL_Access
[Accessed 10 December, 2019]

16. OWASP Top-10 2007 - Information Leakage and Improper Error Handling
[Online] Available: https://www.owasp.org/index.php/Top_10_2007-Information_Leakage_and_Improper_Error_Handling [Accessed 15 October, 2019]

17. Common Vulnerabilities in Web Applications [Online] Available:
https://www.infosec.gov.hk/english/business/other_sywa_1.html
[Accessed 10 December, 2019]

18. Next Generation Threat Prevention, WAF, OWASP Top-10|Tech Brief
[Online] Available: https://www.checkpoint.com/downloads/products/cp-ngtp-waf-owasp-top-10-comparison-tech-brief.pdf [Accessed 12 January, 2020]

19. Technology Editorial- What is Insecure Deserialization? [Online] Available:
https://www.acunetix.com/blog/articles/what-is-insecure-deserialization/
[Accessed 26 December, 2019]

A Survey of Cyber Security Systems: Approaches for Attack Detection, Prediction and Prevention

Jorge Gonçalves
Lusofona University of Porto, Portugal
jorge.oliveira.goncalves@outlook.pt

Hugo Barbosa
Lusofona University of Porto, Portugal
hugo.barbosa@ulp.pt

Abstract. Nowadays the technological advancements that are done daily grow exponentially consequently leading to discoveries being more relevant to improve all the areas that make use of technologies. The purpose of this paper is to centralize some of that progress that can make an improvement in networks through Cyber Security and present the results from an inquiry to a population sample about Cyber Security. It is briefly presented approaches in attack detection, prediction, and prevention. The attack detection topic will be presented on what type of systems exists nowadays, focusing on Intrusion Detection Systems (IDSs). In attack prediction topic will be presented solutions to keep up with the appearance of new forms of attack, allowing to be prepared for then. As for attack prevention, it is done a summary of Social Engineering and Good practice in Cyber Security. It is an essential part of this work an inquire analysis performed in Portugal, prepared in the context of Cyber Security, targeting common users.

Keywords: Cyber Security, Attack Detection, Attack Prediction, Attack Prevention, Good practice, Survey, Inquire.

1 Introduction

Having a network that is able to handle attacks is a must nowadays. To accomplish this, it is crucial to design the network in a way that it is prepared on all fronts. Attack detection, attack prediction, and attack prevention.

This paper's objective it is not to detail every topic under Cyber Security with great detail, but to provide some context information about what exist these days that can enhance security in itself, while also being beginner friendly.

The Cyber Security topic will discuss three sub-topics. In the sub-topic for Attack Detection is presented briefly what systems exist and will be conveyed a summary on Intrusion Detection Systems (IDSs). In the Attack Prediction sub-topic, are going to be reviewed four methods to predict attacks and new forms of attack, those being – Vulnerability Databases, Markov Models, Bayesian Network and Awareness using Twitter. While for Attack Prevention, it will be lightly summarized what Social Engineering is and some good practices to prevent attacks.

10.11228/dpsc.02.01.002

Lastly, is introduced a topic that presents an Inquiry Analysis done in Portugal, which was created with the main focus of gathering data from a population sample regarding their habits on their use of the Internet, the state of cultural knowledge related to cyber security determine how well is the population in general evolving and expose this data to the academic community while serving as a foundation to future related works.

2 Cyber Security Systems

Cyber Security by itself it is the form of protecting computerized network systems against all sorts of attack that gain unauthorized access and may damage the integrity of the system by stealing, blocking access or deleting confidential(private) data or simply by executing dubious tasks. It is ultimately the structuring of systems that are intended to defend a network.

This topic discusses three components of Cyber Security. Attack Detection, Attack Prediction, and Attack Prevention.

2.1 Attack Detection

Even with every prevention and prediction available, it is not always possible to be prepared for all the new techniques of attack, so it is essential to have some sort of defense against it. Having a system or tool that monitories every communication, in and out of the network, and even inside of itself, will lead to an increase in the safety of all the network, ultimately creating a more sustainable system. We highlight the following ones:

- Intrusion Detection Systems.[1]
- Firewalls.
- Anti-virus.

Intrusion Detection Systems

“An intrusion detection system is an application that provides protection from malicious activities or policy violations and generates various rules to defend computer security and this system is relevant for intrusion detection.”[2] Continuous monitorization and application of policies, rules, and verification if and attack signatures if present, require some moderate computational power to maintain this system operational. This leads to the main function of IDSs, which is to warn of suspicious activity is taking place, but it is not its job to prevent it.

Since the use of the Internet of Things (IoT) is growing exponential every day, and systems are more than ever dependent on then, these systems represent a large portion of devices in networks, but with the low computational power that the majority dispose of, they cannot spare processing time. It is crucial to implement new techniques to protect these devices. Recurring to software as a service seems to be one solution for this challenge[3].

In a more generic view, an IDS monitors and evaluates a suspected intrusion once it has taken place, checking its database to detect attack standards. This monitorization is made from both attacks originated from outside and within the systems. Although an IDS monitors and evaluates intrusions, it should be thought of as a replacement for neither a firewall nor a good antivirus program, but instead, as a complement to increase the security of the system, working in pairs with these resources.

There are several techniques to implement intrusion detection systems (IDS), which leads to the following variants.

Variants. [1][4]

- Statistics-based.
- Pattern-based.
- Rule-based.
- State-based.
- Heuristic-based – Machine Learning, Artificial Intelligence, Data Mining.

Choosing the right variant to implementation for each system depends heavily on what constrains that systems may have, so careful planning is required.

2.2 Attack Prediction

Throughout the year there have been countless researchers aiming to find methods to discover what new tools attackers may have developed so that countermeasures can be taken. This section of the paper is focused on presenting information about systems and methods that can be used as tools so that countermeasures to attacks can be taken. If successfully implemented, these systems can lead to gaining a reasonable amount of time so that defensive actions can be made to prevent malicious effects on the networks.

Beneath, is described briefly some of these methods and systems that can help increase considerably how predictions are made towards new manners of attack.

2.2.1 Existing Methods

Vulnerabilities databases.

One of the tools that can be used to gather data, that is going to be inputted into the next presented methods (e.g. through data-mining), are, National Vulnerabilities Database (NVD) which is a U.S. government repository of standards-based vulnerabilities and Common Vulnerabilities and Exposures (CVE) is a list of entries, from is a U.S.

government division, meant to provide reference from publicly known Cyber Security vulnerabilities.[5]

These databases can provide useful data that can be used to train models, Artificial Intelligence programs and Machin Learning Algorithms.

Markov models.

A Markov model is a stochastic model (mathematical object, in which random variables are correlated with or indexed by a set of numbers), that is used to model arbitrarily shifting systems. One premise is that future states depend only on the current state, not relating to events that occurred before it (this being Markov property), they are memoryless. Usually, these models are represented in graphs, allowing for better visual representation and understanding of the problem.[5] Depending on the type of problem or system we have, different Markov models can be employed, which are categorized into four common uses, differing whether every successive state is observable or not and whether the system is to be corrected based on observations made:

Table 1. Different Markov models

	System state is fully observable	System State is partially observable
System is autonomous	Markov chain	Hidden Markov model
System if controlled	Markov decision process	Partially observable Markov decision process

There have been some successful studies related to Cyber Security, where they used Markov models to predict cyber-attacks, proving that these models, even though they were developed a long time ago, they still are a useful tool.[6][7]

Bayesian Network.

Developed in early 1980, Bayesian Networks consists of models that represent knowledge in a form of graphs allowing to reason some conclusion for both discreet or continuous problems, that are based on uncertainties. They are also known as opinion networks, casual networks, and probabilistic dependency graphs.

Throughout the years they have been used to help develop conclusion in many studies, even in Cyber Security prediction, in topics like:

- Combine different sources of Knowledge.[8]
- Models for motivation and psychology of malicious insiders.[9]
- Calculation of the probability of cyber-attacks towards a specific target.[10]
- Prediction of data breaches.[11]

Awareness using Twitter.

With the rapid pace that developments are made, and new forms of attack are discovered, associated with the fact that databases like NVC and CVE have to take their time to ensure that the data that they introduce into their databases is not a false positive, it was encounter a new form of anticipating the appearance of new entries into those databases throw the use of social media platform, Twitter.[12] [13] By analyzing tweets from reliable accounts, that work and investigate malicious software attacks exploitation, it was developed a system that, through the use of Twitter API Stream, can collect live tweets from Twitter and feed then directly to Synapse[13], an threat intelligence program which uses machine learning techniques, allowing it to track the arrival of new exploits mentions before they are introduced to vulnerabilities databases.

Although there are already some threat intelligence systems that can collect data from a wide variety of sources[14], they simply use a keyword filter that restricts the volume of collected information and does not have any sophisticated procedure to select only the relevant data. Synapse was designed to collect data from various sources on the internet, classify it was Cyber Security related content, and aggregate all relevant tweets though a stream clustering algorithm adapted to the context of Cyber Security.[7]

2.3 Attack Prevention

To complement a good infrastructure, it is required that all possible actions that can be done to avoid major damage are implemented, it is here that comes Attack Prevention. This topic will be present briefly two subjects that can, in fact, increase system security by preventing a certain chain of actions.

Social Engineering.

“In a cyber security context, it is primarily used to induce victims towards disclosing confidential data, or to perform actions that breach security protocols, unknowingly infecting systems or releasing classified information.”[15] As mentioned in this quote from Breda F., Barbosa H., Morais T., it is the act of misleading a system user to, unwillingly, compromise the integrity of a system.

Good Practice for Prevention.

From the review and mention, literature was possible to determine some good practice that can significantly increase a system simply by taking preventive measures.[16][17]

- Use of a proper Data Recovery System.
- Keep your systems up to date.
- Instruct your users with basics about Cyber Security.[18]
- Have polices to manage emails, filtering attachments, and potentially misleading sources.

- Have polices to renew passwords, even if they are already considered strong.
- Having Two Factor Authentication for systems that are critical.
- Always report crimes to the cyber fraud complaint center in your counter.
- Among many others.

3 Survey Analysis in Portugal

With the expectation to determine if the common user as evolved alongside the developments in Cyber Security, it was conducted an online survey aiming to get a good population sample from Portugal, with no costs implied, allowing to investigate how well population, in general, is evolving their knowledge regarding Cyber Security and if they are implementing it.[19]

To create and manage the survey it was used Google Forms which allowed the participants to quickly answer and submit their answers anonymously, without the need to use their Google account to authenticate, this way, in a hope, increasing the possible number of participants, since nowadays no one was time. It was also chosen Google Form because of its tools to present and analyze the data extracted from the questions quickly.

On the header of the survey, was given a quick context for why it was created, being that was in the scope of an evaluation for a course unit name Network Complements being lectured in the Lusofona University of Porto. It was also mentioned that the survey was targeted to the public in general that doesn't have responsibilities in managing a computer park, even though it was possible to then to answer, we relied on the professional ethic in a sense that they did not answer. The header also mentioned that the data was going to analyze and was going to be present in a paper about Cyber Security.

In total, there were 258 submissions(participants), being 48.1% (124 of 258) male and 51.9% (134 of 258) female. As for age groups, for ages between 14 and 17 there were 15.1% (39 of 258), from 18 to 25 there were 41.1% (106 of 258), as between 26 and 40 there were 26% (67 of 258) participants, for ages comprehended from 40 to 65 there were 15.1% (39 of 258) and lastly, for the group for participants with 65 and more, it was only possible to get 2.7% (7 of 258).

As for academic abilities, only 0.4% (1 of 258) participants had the fourth grade, for the ninth grade 26.8% (69 of 258), as for the academic level of twelfth grade, there were 36.2% (93 of 258) participants. For higher school education it was possible to get answers from 94 participants (36.6%), from which 24.5% (63 of 258) reported to have Bachelor's degree, 10.9% (28 of 258) participants having Master's degree and 1.2% (3 of 258) Ph.D. Internationally, this academic levels should be equivalent to:

Academic Level in Portugal	Academic Level Internationally
Fourth grade	elementary school
Ninth grade	freshman year
twelfth grade	senior year

This survey was formulated to have two parts not perceptible to the participant. The first part was intended to investigate if the common user, throughout the years with the awareness available online, had begun to implement some of the basics of Cyber Security, like reusing password and not using special characters. For the second part, while still getting some data to evaluate, the main intention was to sub linearly spread some awareness to the participants about some technical terms that sometimes are misunderstood by the common user, in this manner, the options to the answers were quite obvious.

3.1 Population Analysis

Like mentioned above, the survey was intended to be divided into two parts. The first part, focused in this subtopic, was planned to investigate if the population in general has begun to develop any awareness regarding Cyber Security, and if so, if they had started implementing it in their lives, as part of their privacy. Underneath can be observed two tables. One that shows questions, with only yes or no answers, and another table that represents the answers that were provided where the question had more than one choice, with the corresponding percentiles.

From point forward, the questions will be referred to just by their identifier, to increase the comprehension and readability.

Table 2. Question from the survey with yes or no answers related to the first part

Identifier	Question	Yes	No
1	Do you have formation in Cyber Security?	11.2% (29 of 258)	88.8% (229 of 258)
2	Do you know the term Cyber Security?	81.8% (211 of 258)	18.2% (47 of 258)
3	Do you reuse your passwords to do logins?	80.6% (208 of 258)	19.4% (50 of 258)
4	Do you include special characters in your passwords? (Example: ?=”!#)	56.2% (145 of 258)	43.8% (113 of 258)

Table 3. Question from the survey with multiple choices related to the first part

Identifier	Question	Work	Entertainment	Work and entertainment	Don't use
5	In what context do you use computers and/or smartphones?	2.3% (6 of 258)	11.6% (30 of 258)	84.5% (218 of 258)	1.6% (4 of 258)

For starters, questions 1 and 2 were made to understand how familiar participants were regarding some of the basics in Cyber Security and it was positive to see that, even though only 11.2% (29 of 258) had formation in this area, a larger portion of then, 81.8% (211 of 258), affirmed knowing the term Cyber Security. Although knowing the term doesn't mean that they, in reality, know anything about it, analysing the result from question 4, 56.2% (145 of 258) yes and question 3, 19.4% (50 of 258) no, can be deducted that some of the basics principals, the ones asked in those questions, are being applied.

The reuse of passwords, question 3, like mentioned by Don Norman in one of his books [20], Chapter 3 - Memory Is Knowledge in the Head, is something that even security professionals admit to do, but comes with a great risk since having one password compromised can lead to the loss of privacy and integrity in multiple systems. This is even a greater threat when corelated with question 5. Assuming that companies leave to the user the choice of their passwords, this can lead to then reusing one of their passwords which can already be compromised, conducting to introducing a vulnerability in the company network. This is special alarming when in 84.5% (218 of 258) participants affirmed using computers and smartphones for both work and entertainment.

Using special characters can exponentially increase the strength of a password, particular when this one is targeted by dictionary attacks or even brute force[21]. The use of special characters accomplishes this by breaking the sequence of sentences, when the user creates a password with words, introducing a strange element that algorithms will not be able to identify easily. It was optimistic to see that 56.2% (145 of 258) affirmed using special characters, but there is still an alarming large percentile that doesn't do it, 43.8% (113 of 258).

Table 4. Table that relates the educational level with both question 3 and 4.

Identifier	Answer	Fourth Grade	Ninth Grade	Twelfth Grade	Bachelor	Master	Ph.D.
3	Yes	0% (0 of 25)	20.2% (52 of 258)	28.7% (74 of 258)	22.5% (58 of 258)	8.1% (21 of 258)	1.2% (3 of 258)
3	No	0.4% (1 of 258)	7.0% (18 of 258)	7.4% (19 of 258)	1.9% (5 of 258)	2.7% (7 of 258)	0% (0 of 258)
4	Yes	0% (0 of 258)	12.8% (33 of 258)	14.3% (37 of 258)	9.7% (25 of 258)	6.2% (16 of 258)	0.8% (2 of 258)
4	No	0.4% (1 of 258)	14.3% (37 of 258)	21.7% (56 of 258)	14.7% (38 of 258)	4.7% (12 of 258)	0.4% (1 of 258)

Arranging the data retrieved from the survey in academic groups and analyzing question 3, we can see that even with higher education participants still persist in reusing their passwords. In question 4, only above the Master's degree it is determined that a larger percentage of participants do include special characters in their passwords, which may indicate a higher level of awareness.

Analyzing the results from both questions, it is possible to conclude, that having a higher academic level doesn’t necessarily mean that participants are more aware of the potential threats.

Table 5. Table that relates the group ages with both question 3 and 4.

Identifier	Answer	14-17	18-25	26-40	40-65	65+
3	Yes	11.2% (29 of 258)	33.3% (86 of 258)	24% (62 of 258)	9.7% (25 of 258)	2.3% (6 of 258)
3	No	3.9% (10 of 258)	7.8% (20 of 258)	1.9% (5 of 258)	5.4% (14 of 258)	0.4% (1 of 258)
4	Yes	6.2% (16 of 258)	17.4% (45 of 258)	11.6% (30 of 258)	8.5% (22 of 258)	0% (0 of 258)
4	No	8.9% (23 of 258)	23.6% (61 of 258)	14.3% (37 of 258)	6.6% (17 of 258)	2.7% (7 of 258)

With the information now organized into the group ages from the survey, it is possible to determine, relatively to question 3, that the answers, in general, are quite negative for the state of Cyber Security nowadays, where only the group from 18-25 seems to have a small indicator, 7.8% (20 of 258), that some participants are becoming more aware of small changes that they can make to increase security. In question 4 we can observe that there are other indicators in both 14-17 and 18-25 that may suggest that some representatives from these groups are more aware, which may lead to a small portion of future generations being more conscious.

It is to notice that participants with 65+ may have their privacy vulnerable since in question 4 none of the participants affirmed including specials characters in their passwords.

The most important objective of this survey was to determine if the common user reuses his passwords (question 3). This was the focus since nowadays, with all the data breaches involving personal data belonging to their user base, from companies that have authentication systems, many times users get their password unveiled and don’t even get notified, leaving all their privacy exposed and potentially companies network systems compromised. It was also wanted to discover if they did include any special characters in their passwords (question 4) since this can interfere considerably with dictionary attacks.[22]

3.2 Common Technical Terms

The inquiry second part's main objective was to sub linearly educate the participants about what are some of the technical terms used in Cyber Security and what they mean. With this in mind, the questions were formulated to be multiple choice and with 4 possible answers, one of those being the right one.

The correct answer was formulated based on information acquired from an online curse from the Nacional Centre of Cybersecurity – Portugal.[18]

Bellow, it is presented a resume of all the participant's answers, where all the wrong answers were agglomerated into just one column.

Table 6. Questions from the survey related to the second part

Identifier	Question	Correct	Wrong
6	What is a Malware?	89.1% (229 of 258)	10.9% (29 of 258)
7	What is a Ransomware?	80.6% (208 of 258)	19.4% (50 of 258)
8	At what does Phishing refer to?	83.1% (212 of 258)	16.9% (46 of 258)
9	At what does the concept of Malvertising refer to?	75.2% (194 of 258)	24.8% (64 of 258)

From this data, it is possible to observe that terms more commonly used, like Malware and Phishing, have a higher Correct answer percentage, but when it comes to Ransomware and Malvertising, participants seam to still don't know about then, which suggest that some social awareness could provide some knowledge.

3.3 Acquired Results

Analyzing the answers obtained in this inquiry, it is possible to conclude that the population, in general, is evolving, overall, in a somewhat positive way considering the fast pace from technological developments and how humans must adapt to keep up with it.

Ultimately, there is still a margin for improvement. The fact that only 11.2% (29 of 258) participants have formation in Cyber Security, associated with the facts that 80.6% (208 of 258) reuses their passwords, 56.2% (145 of 258) don't use special characters, that the majority of the next generations doesn't protect their online security properly, suggest that, at an educational level there is still some enhancements that can be done, leading to conclude that it would be a high benefit, for both individuals and companies, to invest in teaching Cyber Security earlier in academic life of children's, this way making the population more cautious on their daily use of technology, that being in the context of work, entertainment or both.[19]

4 Conclusion and Future Work

Towards accomplishing a sustainable and secure network system and more protected users, it is essential that all intervenient, system and users, are adequately prepared to ensure this. Through the combination of all topics discussed above, seems to be the most advantageous approach when creating a system like so. A combination of, the most adequate Intrusion Detection Systems, updated information about discovered forms of attack and user knowledge will certainly culminate in a sustainable network. Inquires like this yield great information about the state of the general knowledge of the population and as observed by the results, it could be gained a lot by introducing Cyber Security principals earlier in academic carriers.

As for future work, it is intended to continue this study, looking to promote awareness among users to such an important and relevant area, and also seeking to conduct studies with more extensive samples.

References

1. Hung-Jen Liao, Chun-Hung Richard Lin, Ying-Chih Lin, Kuang-Yuan Tung.: Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications (2013)
2. Heena Batra & Gaurav Gautam.: An Improved Intrusion Detection System Using Clustering Technique in Data Mining. https://edupediapublications.org/journals [Las accessed 16-12-2019] (2018)
3. Geethapriya Thamilarasu, Shiven Chawla.: Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things. University of Washington Bothell (2019)
4. Sumeet Dua and Xian Du.: Data Mining and Machine Learning in Cybersecurity. Auerbach Publications (2011)
5. Harold Booth, Doug Rike and Greg Witte.: The National Vulnerability Database (NVD): Overview. ITL Bulletin (2013)
6. Anna Sperotto, Ramin Sadre, Pieter-Tjerk de Boer, and Aiko Pras.: Hidden Markov Model Modeling of SSH Brute-Force Attacks. IFIP International Federation for Information Processing (2009)
7. Subil Abraham, Suku Nair.: A PREDICTIVE FRAMEWORK FOR CYBER SECURITY ANALYTICS USING ATTACK GRAPHS. International Journal of Computer Networks & Communications (IJCNC) Vol.7, No.1. (2015)
8. Sabarathinam Chockalingam, Wolter Pieters, André Teixeira, and Pieter van Gelder.: Bayesian Network Models in Cyber Security: A Systematic Review. Proceedings of the Nordic Conference on Secure IT Systems (2017)
9. Elise T. Axelrad, Paul J. Sticha, Oliver Brdiczka, Jianqiang Shen.:A Bayesian Network Model for Predicting Insider Threats. IEEE Security and Privacy Workshops (2013)
10. Ahmet Okutan, Shanchieh Jay Yang, Katie McConky.:Forecasting Cyber Attacks with Imbalanced Data Sets and Different Time Granularities. Rochester Institute of Technology, Rochester, NY, USA (2018)

11. Lisa de Wilde.:A Bayesian Network Model for Predicting Data Breaches. University of Twente in cooperation with Delft University of Technology (2016)
12. Ba-Dung Le, Guanhua Wang, Mehwish Nasim, M. Ali Babar.:Gathering Cyber Threat Intelligence from Twitter Using Novelty Classification. University of Adelaide (2019)
13. Fernando Alves, Aurélien Bettini, Pedro M. Ferreira, and Alysson Bessani.: Processing Tweets for Cybersecurity Threat Awareness. Faculty of Sciences, University of Lisbon – Portugal (2019)
14. SpiderFoot, Open Source Intelligence Automation. http://spiderfoot.net/. [Last accessed 15-12-2019].
15. Breda F., Barbosa H., Morais T. .:Social Engineering and Cyber Security. INTED 2017 Proceedings (2017)
16. Ms M Lakshmi Prasanthi, Tata A S K Ishwarya.: Cyber Crime: Prevention & Detection. International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 3 (2015)
17. Valdemar Sousa.: A Review on Cyber Attacks and Its Preventive Measures. Proceedings of the Digital Privacy and Security Conference (2019)
18. Cidadão Ciberseguro.: Centro Nacional de Cibersegurança – Portugal (2019)
19. Noam Ben-Asher, Cleotilde Gonzalez.: Effects of cyber security knowledge on attack detection. Computers in Human Behavior 48. (2015).
20. Donald A. Norman.: The Design of Everyday Thing. Basic Books(AZ) (2013)
21. Eugene H. Spafford.: Preventing Weak Password Choices. Computer Science Technical Reports, Purdue University (1991).
22. Kouroush Jenab and Saeid Moslehpour.: Cyber Security Management: A Review. Business Management Dynamics Vol.5, No.11 (2016)
23. Martin Husák, Jana Komárková, Elias Bou-Harb, and Pavel Čeleda.:Survey of Attack Projection, Prediction, and Forecasting in Cyber Security. IEEE Communications Surveys & Tutorials (2018)
24. George Onoh.: Predicting Cyber-Attacks Using Publicly Available Data. Bowie State University (2018)
25. Lisa de Wilde.:A Bayesian Network Model for Predicting Data Breaches. University of Twente in cooperation with Delft University of Technology (2016)
26. Threat Analysis - Intelligence Monitor – Track Cyber Threats. https://www.surfwatchlabs.com/threat-intelligence-products/threat-analyst. [Last accessed 15-12-2019].
27. Geethapriya Thamilarasu, Shiven Chawla.: Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things. University of Washington Bothell (2019)
28. Prabaharan Poornachandran, M. Nithun, Soumajit Pal, Aravind Ashok Nair, Aravind Ajayan.: Password Reuse Behavior: How Massive Online Data Breaches Impacts Personal Data in Web. Innovations in Computer Science and Engineering (2016)
29. Nabie Y. Conteh1, Paul J. Schmick.: Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, Vol 6(23) (2016)

A Survey of Cyber Security Systems: Approaches for Attack Detection, Prediction, and Prevention

Vera Oliveira

Lusófona University of Porto, Portugal
a21801187@mso365.ulp.pt

Abstract. Nowadays, cyber security is a daily part of life for organizations, governments and the general public of all ages throughout the world. A firm with weak cyber security imposes negative externalities on its customers, employees, and other firms tied to it through partnerships and supply chain relations. Due to the difficulty of identifying and punishing malicious actors, and the ever-greater interconnectedness stemming from the intensified use of the Internet, malicious cyber activity is becoming more and more widespread. One of the main points of it is the globalization and human that factor have become essential to the cyber security proper use and application policies. To this effect, this paper presents a survey of cyber security approaches on the three major topics, attack detection, prediction, and prevention. This paper also reviews the methodologies, strengths, and weaknesses for these approaches. Furthermore, this paper will help predict future cyber attacks and help with preventing from happening again.

Keywords: Cyber Security, Cyber attack, Cyber attack Detection, Security, Threats, Prediction, Prevention, Countermeasure

1 Introduction

The existing approach to cyber security has been mostly reactive. For example, traditional mechanisms to defend against malware are based on matching attacks against known signatures. As new strains of malware are discovered, signatures are added to the list of known attacks. This approach works only if the volume and variety of attacks are low. With the increase in the number of attacks, however, by the time a new attack has been identified, significant damage may already have been done. [1] One of the most problematic elements of cyber security is the quick and constant evolving of cyber risks. Therefore, this paper will help gain an understanding of the threat, explain it and shed some light on how to detect, predict and prevent from one.

10.11228/dpsc.02.01.003

2 Cyber Attack

Cyber attack is the action that attempts to bypass the security mechanisms of computer systems. So, they are any set of actions that threatens the integrity, availability, and confidentiality of network resources. [2]

It’s a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Usually, the attacker seeks to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of anything that has value to the organization or individual. [3]

Cybercrime has increased every year as people try to benefit from vulnerable business systems. Cyber threats can also be launched with ulterior motives. Some attackers look to obliterate systems and data as a form of “hacktivism”. [4]

Cyber security concerns with the understanding of the surrounding issues of diverse cyber attacks and devising defense strategies that can preserve confidentiality, integrity, and availability of any kind of digital and information technologies. [5]

2.1 Purpose and Motivations

Sometimes we ask what motivates cyber attackers, and why they do it. Understanding the motives behind a targeted attack is important because it can help pinpoint what to protect and how to protect it. A simple profit motive scenario can be a smokescreen hiding a different, deeper kind of attack, such as:

Espionage: usually aimed at gathering information from the victim. It’s a clandestine activity and the attackers strive to avoid detection, at least until they achieve their goal. These are also among the most persistent often continuing the attack vector even after they’ve been detected.

Profit: direct financial gain a common profit-driven attack in use today and include theft and resale of credit card information or ransomware.

Ideological: someone that wants to harm the reputation, deny services to customers, or sabotage the systems to further their propose or eliminate perceived threats to the environment, for example, a frustrated ex-employee.

Information Theft: when the aim is to acquire information owned by the target and/or stored in the network. This information can be in form of customer information, business-critical information or even intellectual property.

Several others self-explanatory purposes for example extortion, revenge or sabotage. [6]

2.2 Common types of cyber attacks

Malware: is a term used to describe malicious software, that breaches a network through a vulnerability, most typically when a user clicks on a dangerous link or email with an attachment that will lead to risky software installation. Once inside the system, the malware can disrupt certain components of the network and block the access to the system, it can also obtain information by transmitting data from the hard drive or installing additional harmful software.

Phishing: is the practice that gathers sensitive information like login credentials, credit card numbers, bank account numbers or other financial information by masquerading itself as a legitimate site. This type of scams creates a sense of urgency to manipulate users. [7]

Denial-of-service (DoS): it floods the systems, servers or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests or simply crashes.

Man-in-the-middle attack: also known as eavesdropping attack, occur when an attacker inserts themselves into a two-party transaction. Once in the middle, they can access, read and change secret information without keeping any trace of manipulation. [8]

Brute force attack: comprises repeated attempts to gain access to protected information until the correct key is found, for example, passwords.

Social engineering: is the technique used to gain unauthorized access to information through human interaction, also known as human hacking. Engebretson [9] defines social engineering as “one of the simplest methods to gather information about a target through the process of exploiting a human weakness that is inherent to every organization.” The attack aims at manipulating victims to divulge confidential information.

Furthermore, there are two types of attacks scenario:

Un-targeted attacks: which attackers indiscriminately target as many devices, services or users as possible. The attacker doesn’t care about the victim is as there will be several targets.

Targeted attacks: the attacker has a specific interest in your business or has been paid to target you. A targeted attack can often be more damaging than un-targeted one because it has been specifically tailored to attack your systems, processes or personnel, in the office or at home. [10]

3 Cyber Attack Detection

Cyber attack detection is a common attack mitigation technique. It involves responding to an abnormal connection to report the presence of an attack pattern or profile in a network. With the ever-increasing threat environment, no matter what level of protection a system may have, it will get compromised given a greater level of motivation and skill. A defense in layers strategy should be deployed so when each layer fails, it fails safely to a known state and sounds an alarm. The most important element of this strategy is timely detection and notification of a compromise. Intrusion detection systems (IDS) are utilized for this purpose, it is the process of identifying an intrusion or attack signature in a continuous flow of connections. [11]

3.1 Analysis Approach

Currently there are three basic approaches to cyber attack detection, mostly used to make the engine analysis by processing the data in order to identify cyber attacks.

Misuse Detection: misuse detectors analyze system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack. This approach is concerned with finding intruders who are attempting to break into a system by exploiting some known vulnerabilities. The basic idea is to use the knowledge of known attack patterns and apply this to identify attacks in various sources of data being monitored. Therefore, the efficacy of the system relies heavily on the thorough and correct construction of this knowledge base.

Anomaly Detection: is the identification of rare items, events that raise suspicions by differing significantly from the majority of the data. [12] Anomalous data can indicate critical incidents, a glitch or an attack.

Specification-based Detection: specification-based approach of misuse detection works just like the existing anti-virus software. [13] The specification-based techniques in this approach are used for reducing the number of false alarms. [14] But they are not as effective as anomaly detection, especially when it comes to network probing and denial-of-service attack.

3.2 Cyber Attack Detection Systems

Cyber Attack Detection Systems (CADS) is a software that automates the process and detects possible cyber attacks. They have three major security functions: monitor, detect and respond to unauthorized activity by company insiders and outsiders attackers.

Antivirus Software: is a computer software used to detect, identify, prevent and remove malicious software. [15] This type of programs is not always effective against new viruses, the reason is that before releasing them, the virus designers test them on the major antivirus applications.

Firewalls: is a network security system for monitoring and control over the incoming and outgoing network traffic based on predetermined security rules. [16] A firewall typically establishes a barrier between a trusted, secure internal network and another external network, it will filter traffic between these two and controls network traffic in and out of that single machine. The attempt to bypass the firewall rules may result in the creation of an open channel for attackers to attack. [15]

Haystack: it was developed for the detection of cyber attacks in multi-user Air Forge computer system. To detect cyber attacks the system employs two methods of detection anomaly detection and signature-based detection. [17]

Later haystack was implemented on an Oracle database management system running on an IBM-AT clone. Haystack periodically downloaded the audit trail file from the target Standard Base Level Computers (SBLC), this file contained the session duration, number of files opened, number of pages printed, number of CPU resources consumed in the session, and number of sub-processes created in the session. In total, the system included more than 30 features for each session because there was no notion at the time of which feature were most effective in detection intrusions. [18]

MIDAS: although old, Multi Intrusion Detection and Alerting System (MIDAS) was designed and written to perform rule-based cyber attack detection. For developing, compiling, and debugging the rules. [19] It was designed to take data from Docmaste's answering system audit log. This data was organized, used to construct session profiles, and then compared to user profiles of normal behaviour. MIDAS combined statistical anomaly detection with expert system rule-based approaches. [18]

IDS: is a device or software application that monitors and analyse a network or system for signs that malicious activity are taking place to either infiltrate or steal data from the network. IDS compares the current network activity to a known threat database to detect the kind of behaviour like security policy violations, malware, and port scanners. IDS requires a human or system to verify the results to determine what actions to take next.

4 Cyber Attack Prediction

To predict the future, you are restricted to examining the past. Any event can be predictable if it occurs in a non-random way, allowing to extract random contexts that may be based on learning and identifying associations. Prediction comprises two types of activities: on one hand, forecasting or prediction in the narrow sense, and anticipation on the other. The key distinction between both is that in the former, current actions are based on past behaviour, while in the latter, predictions about the future guide current actions. With this anticipatory processing, benefits include an increase in accuracy, speed or maintenance of information processing. [20]

4.1 Predictive analytics and machine learning

Predictive analytics is the art of building and using models that make predictions based on patterns extracted from historical data. Some peculiarities of cyber security also make it more challenging to apply machine learning and the evolution of attacks that requires learning to be incremental. Machine learning is often used to build predictive models for classification and to cluster data, this technique can be grouped into supervised, unsupervised, and hybrid techniques.

One of the challenges in cyber security context is that machine learning models can themselves be attacked. [21] Through a carefully attacks, attackers can gain an understanding of the internal state of a machine learning model, which allows them to attack more effectively in the future.

4.2 Vulnerability prediction

In other words, vulnerabilities are weaknesses, flaws that can be exploited by threats to cause harm to an asset. Given that not all vulnerabilities are of equal impact and if resources are limited, the manager needs to prioritize on which patches to create or to deploy. Vulnerability prediction can be of assistance in this task by predicting the kinds of vulnerabilities that exist in a system and the risk of them being exploited. One way to know almost all the vulnerabilities that exists is to use NVD, that is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). [22]

4.3 Honey Implementation

Honeypot is a computer security mechanism set to detect, deflect, or counter the attempts at unauthorized system. Generally, a honeypot consists of data, and it appears to be a piece of real information and it would be in a part of the system but actually isolated and monetarized, as it seems to contain resources or value information to the attackers, it attracts their attention.

Two or more honeypots on a network form a honeynet. They are used for monitoring a larger and more diverse network. [23]

5 Cyber Attack Prevention

Prevention of attacks is a proactive activity that identifies and responds to potential threats in a network quickly. Most detection approaches are reactive and are only applied after much damage has been done on the impact zone. Several intrusion prevention systems (IPSs) have been proposed as a tool for improving cyberspace security. Cybernetic prevention has the primal act of restricting, controlling, removing or preventing the occurrence of cyber attacks in a computer system. Cyber prevention is responsible for detecting irregularities in the activities of the Internet user. [24]

IPS: an Intrusion Prevention System live in the same area of the network as a firewall, between the outside world and internal network. this proactively deny network traffic based on a security profile created if that packet represents a threat it will be dropped before, they reach their target. Just like IDS, it requires that the database gets regularly updated with new data threats.

Prevention Tips: falling victim to cyberattacks can be devastating, it causes downtime, the damaged reputation of the firm. Aside from the more conventional solutions, like the anti-virus and the firewall, there are simple, economical steps to reduce the risk:

1. Train employees in cyber security principles.
2. Make backup copies of important data and information.
3. Control physical access to your computers and network components.
4. Limit employee access to data and information and limit authority to install software.
5. Regularly change passwords.
6. Require individual user accounts for each employee.
7. Regularly update antivirus and antispyware software and applications as they become available.

6 Detecting and Defending against Phishing attacks

One of the most persistent security challenges is phishing. This is true for both organizations and individuals. Whether gaining access to credit card information, security passwords, or any other sensitive information, hackers can use different techniques, such as social engineering, emails, phone calls, and other forms of communication, to steal data. This opens businesses as worthwhile targets since they have valuable data on hand. Evidence that it is necessary to include the human factor in security modelling. These are attacks in which, typically, the victim is deceived to give out secret information enabling access to a given resource [25]

6.1 Common way of cyber criminal attacks

- Sending a link through email that opens a malicious website.
- Placing a trojan in the target's computer through an email attachment.
- Creating a spoofed email to look as reputable as possible and tricking the receiver.
- Impersonating a vendor or IT department and calling via phone.
- A technique where content with malicious intent is injected into the company's website to obtain passwords.
- Hackers positioning themselves in the middle of the company and their customers to capture any and all information transmitted between them.
- DNS-based phishing attack that forces people into a malicious website when they try to visit the target website.

6.2 How to defend against phishing attacks

- Use an SSL certificate on your website to protect all information transmitted between the web server and the visitor's browser.
- Provide proper and regular training to employees about phishing, how to identify it, and what to do when they suspect an attack.
- Ensure that all security tools, protocols, and controls are up to date. Also, take note of new developments in the IT industry about tools and new types of attacks, to be able to adapt to the company's defenses.
- When a payment page is needed for your website, make sure to use a securely hosted page. This is the best practice in order to secure credit card information being transmitted over the internet.
- Create a filter that can detect the most common types of spam and phishing attacks. This should be also able to identify attachments and filter malicious ones.
- Use an antivirus solution for each endpoint device, as well as the entire network.
- Encrypt the sensitive data of the company so they are difficult to open even when stolen.
- Use a web filter in order to block malicious websites from even opening on your network.
- Disable HTML email feature within the organization, which will reduce the risks of phishing attacks.
- Make sure to require proper encryption for all employees who telecommute or work remotely.

7 Conclusion

Despite all the efforts that have been done in the last three decades to prevent widespread dissemination of insecurity in the Internet traffic by the most important companies (Kaspersky, Microsoft, Symantec, among others), the battle is yet to be won. Reading their monthly newsletters gives us an accurate idea of the huge challenge they're facing today. The rate of solved security threats every month is much lower than the patches they send their customers to "remain secure" today. The main idea prevailing is "You remain secure until you press the ENTER key" or "LOG IN" in an internet URL.

References

1. Michael Weiss.: From prediction to anticipation of cyber attacks. IJBT (2018).
2. Shailendra Singh and Sanjay Silakari.: A Survey of Cyber Attack Detection Systems. In: International Journal of Computer Science and Network Security, VOL.9 No.5, (2009).
3. INTERNATIONAL STANDARD.: ISO/IEC 27000:2009(E).
4. What Are the Most Common Cyber Attacks https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html, last accessed 2019/12/15.
5. Julian Jang-Jaccard, Surya Nepal.: A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80 (2014).
6. Know your cyber enemy by IBM Security, https://www.ibm.com/downloads/cas/ZDEYR18P, last accessed 2019/12/17.
7. Andreea Bendovschi.: Cyber-Attacks – Trends, Patterns and Security Countermeasures. Elsevier (2015).
8. Avijit Mallika, Abid Ahsanb, Mhia Md. Zaglul Shahadata and Jia-Chi Tsouc.: Man-in-the-middle-attack: Understanding in simple words. International Journal of Data and Network Science (2019).
9. Engebretson P.: The basics of hacking and penetration testing: ethical hacking and penetration testing made easy. Elsevier (2011).
10. Great Britain, Government Communications Headquarters, Computer Emergency Response Team UK.: Common Cyber Attacks: Reducing The Impact. BIS (2015).
11. N. B. Aissa, M. Guerroumi.: "Semi-supervised statistical approach for network anomaly detection". Procedia Computer Science, (2016).
12. Zimek, Arthur, Schubert, Erich.: "Outlier Detection". Encyclopedia of Database Systems, Springer New York, (2017).
13. Jamal Raiyn.: A survey of Cyber Attack Detection Strategies. International Journal of Security and Its Applications Vol.8, No.1 (2014).
14. R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang, S. Zhou.: "Specification-based anomaly detection: a new approach for detecting

network intrusions". In: Proceedings of the 9th ACM conference on Computer and communication security, pp. 265– 274, Washington D.C., USA, (2002).

15. Martellini, Maurizio, Malizia, Andrea.: Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges: Threats and Counter Efforts. Springer. (2017).
16. Todd Lammle.: CCNA Routing and Switching. Complete Review Guide. John Wiley & Sons, (2016).
17. Stephen E. Smaha. Haystack: An intrusion detection system. In proceedings of the IEEE Fourth Aerospace Computer Security Applications Conference, Orlando, FL, USA, (1988).
18. Rebecca Gurley Bace.: Intrusion Detection.1st edn. Sams Publishing. Indianapolis, (2000).
19. Michael M. Sebring, Eric Shellhouse, Mary E. Hanna, R. Alan Whitehurst.: Expert systems in intrusion detection: A case study. In: Proceedings of the 11th National Computer Security Conference, pages 74.81, Baltimore, Maryland, (1988).
20. Andreja Bubic, D. Yves von Cramon, Ricarda I. Schubotz.: Prediction, Cognition and the Brain. Front Hum Neurosci, (2010).
21. Barreno, M, Nelson, B, Joseph, AD, Tygar.: JD: The security of machine learning. Machine Learning, 81, pp. 121–148 (2010).
22. National Vulnerability Database, https://nvd.nist.gov/#, last accessed 2019/12/17.
23. Mr.S.Thanigasalam, Dr.M.Savitha Devi.:Finding Attackers Details to Solve Security Issues Using Honeypots Technique. Shanlax International Journal of Arts, Science and Humanities (2018).
24. Valdemar Sousa.: A Review on Cyber Attacks and Its Preventive Measures. Proceedings of the Digital Privacy and Security Conference (2019).
25. Markus Jakobsson.: Modeling and Preventing Phishing Attacks. Financial Cryptography, (2005).

Review of cyber threats on Educational Institutions

Jorge Pinheiro

Lusofona University of Porto, Portugal
jmiguelpinhiero@hotmail.com

Abstract. The aim of this paper is to review about the cyber threats on educational institutions. The paper will focus on summarizing the threats and explaining the problems that cyberattacks can cause, the origin of the attacks and what motivations can the hackers have to do this sort of things. Nowadays, the percentage of attacks to educational institutions is going up and there are many threats to institutions and even more dangers behind them. This paper will also show some suggestions to this problem that keeps terrifying the educational institutions in the days that we live and how to try to prevent them.

Keywords: cyber threats, educational institutions, attacks, dangers, hackers, prevention.

1 Introduction

Many of the day-to-day IT risks originate within the company or institution in question. They may consist of leaks of information from their employees, students or even teachers, which intentionally or involuntarily disclose passwords, sensitive information or actions from people with bad intentions within the institution, such as a student who wants to take advantage of their access and knowledge to gain entry into college networks or an employee who wants to harm something because he was fired, and forgetfully, the institution did not delete that person's data.

Educational institutions are a real gold mine for cybercriminals [1]. These store thousands of information from each student, teacher and staff. Bank accounts, addresses, school transcripts and other valuable data. Formerly the institutions were not attacked, but today that has changed.

There is a doubt that brings concern to universities, schools and other educational environments and it’s why the area of education is so hit by cyber criminals, and one of the explanations is in the public that frequents these institutions. The fact that some students and teachers use computer labs and there is a risk of misuse is one of the main factors. Even if unintentional, a simple student can undermine the systems and information of an institution for a slight failure or bad use of their mobile phone for example. This same student when connecting to web pages or giving permissions on untrustworthy websites may be opening doors for hackers to enter.

10.11228/dpsc.02.01.004

In an educational institution there are hundreds of students, dozens of teachers, dozens of employees and collaborators, and the greater the number of people, the riskier and harder to monitor the cyber security gets.
Another of the many risks that we will talk about is the USB (Universal Serial Bus) flash drives brought, for example, by a student or teacher that is very useful for both of them to store important files, but that is one of the main transports for the entry of viruses.
One of the most important security strategy points is to control network access and only let each type of user who enters the network see the information to which they are only entitled and allowed. This lowers the likelihood of malware intrusions or infections that can damage networks, systems, equipment, and devices.

Today, universities, colleges, and schools track digitally absences, attendance, and grades as well as confidential student and parent documents. This information is increasingly vulnerable and easy to attack since there is no truly effective data protection program.

In section 2 of this paper we will talk about cyber threats in educational institutions, with an example of a teenager who entered two softwares from two different companies, which kept confidential data from the school where he used to study and also will be presented different types of threats and their definition.

In section 3 will be covered about what can be done to prevent any cyber threat and includes some tips on how to protect the network of institutions and reduce the risk of attack.

In terms of origins and motivations, some important aspects of why hackers break into networks and steal information will be summarized.

2 Cyber Threats

Educational institutions today face unique security challenges unseen in other sectors, so cyber security must be a priority. In addition, these institutions have a large and complex network with a large number of switches, routers and single users, making keeping the system secure from cyberattacks is an extremely difficult task [2]. IT departments must address these risk areas and find ways to mitigate threats. A university, for example, may contain thousands of users. These users may enter the system through older, less protected hardware such as a computer or a mobile phone that may not have the features required to install the latest software versions to remain protected, thus leading to a high vulnerability to attack.

While the education sector continues to grow, more institutions continue to evolve and opt for digital solutions to check a student's performance, schedules or even monitor tasks and organize them, which is of great importance to hackers. While institutions continue to collect immense amounts of student information, the responsibility to keep this type of information secure also increases [3]. As a result, information carries a great risk of being attacked in a variety of ways, and hackers can find various ways to break into systems to gain access to anything that is valuable.

An example of cyber threats is the case of Bill Demirkapi who a few years ago, when he was in tenth grade, he was a typical hacker. A bored teenager who broke into the school network where he was going to change his grades [4]. At the DEFCON conference in Las Vegas [5] (one of the largest hacking conventions in the world), he presented his three-year breakthrough after-school hacking, which began when he was still a student at the school.

Demirkapi explored two types of software sold by two companies, Blackboard [6] (technology education company) and Follett [7] (company that deals with vital information), which were used at the school where he went. In both cases, he encountered serious bugs that could give a hacker deep access to a student's information. In the case of Blackboard, Demirkapi found 5 million vulnerable student and teacher data, including grades, balance to spend on school, schedules, password hashes, and photos. He himself stated that if he were not a young man motivated by his curiosity, he could so easily enter corporate databases, his story does not quite demonstrate the security that exists in these companies, which have millions of personal information from each student.

“The access I had was pretty much anything the school had. The state of cybersecurity in education software is really bad, and not enough people are paying attention to it”.

The bugs that Demirkapi found in both companies were very common on websites, including SQL injection and cross-site scripting vulnerabilities. Detailing each company, in the case of Blackboard, the bugs found gave full access to a database with 24 categories of information, with everything from phone numbers to bus routines done. The data belonged to over 5000 schools, with 5 million total data, including students, teachers and other staff. In the case of Follett, the bugs found in this software gave the hacker access to data such as grade point average, number of suspensions and passwords, which unlike Blackboard, were kept unencrypted. When Demirkapi gained access to this level of information, he knew the risks of fraud and abuse that prohibited gaining unauthorized access to a company's network.

With this he asked a friend for permission to verify that the data he had matched the data he had obtained. Demirkapi neither explored nor counted how much vulnerable data he had discovered as he did with the Blackboard company. However, the companies were grateful that he found these bugs, and reported them, to fix all problems they encountered. But let's imagine that Demirkapi, instead of doing what he did to help companies, kept the data. All the data found could have fallen into the hands of others who could use this sensitive data to make money.

In the next topic, we'll talk about some types of threats that exist that can cause serious damage to institutions.

2.1 The real danger for educational institutions

Technology developments and constantly changing transformations open many possibilities for educational institutions, but also increase the vulnerability and risk of hacker attacks [8]. Misuse or involuntary mistakes made by someone within the institution is one of the major problems seen by the values above. This leads us to think that institutions should take security measures and inform students, teachers and staff of the great risk of misuse of technological devices and devices. With each passing year, it can be said that the compromise of personal data and sensitive data in institutions increases compared to previous years.
Schools, colleges, and other educational establishments store a wealth of valuable student, parent, and staff information, including personal information, financial data, and even study materials.

Each year schools make the transition to the cloud and the security is left behind. The adoption of cloud technologies means security teams must be able to monitor suspicious and malicious activity from external threats.
The beginning of the school year means that thousands of students and staff will return to the institutions' cloud environments. It also means that thousands of pieces of information will enter and leave databases, which could lead to hackers having more reason to attack any of these institutions.

Educational institutions have a complex and distributed IT (Information Technology) architecture. Due to be a space open to all, there is a great diversity of public, which leads to having to provide zones of different virtual environments. This also means that everyone who is connected needs to be safe. For example, in a teachers' room, students, parents, staff and visitors to institutions cannot have access and can connect to that area. However, in other environments such as libraries, they are spaces that were made for exchanging information and ideas, so there will be a large flow of visitors and users coming in and out of the system. These environments pose a greater risk to the institution due to user behavior, whether intentional or unintentional. Misuse of computers, mobile phones, tablets and pens could pose serious risks such as damage to equipment, malware and the entry of users who should not have access.

But there is another problem, which are the holes in systems that make it easy to steal information or even change that sensitive information. Different types of data such as administrative, financial, and student records can easily be stolen or altered by anyone unknowingly. Therefore, in areas with high data transfer and little control over users, it is necessary to have devices or technological devices that can provide access, but not forget security.

There are different types of threats that are worrying and may cause disruption to educational institutions. Next, we will talk about some types and in the following topic, tips on what to do to protect institutions will be covered [9][10][11][12]:

- **Malware** [9][10]: This is the same as malicious software. It's any piece of software that was created to damage devices, steal information and usually create a great deal of confusion. There are different types of malware like worms, trojans, botnets and adware.

- **Worms**: Can infect a network of devices locally or over the internet using the network interface. Uses each machine affected to infect other people.

- **Spyware**: This is malware that was created to spy on a person. Hides in the background and takes notes of what this person does online, can include passwords, credit card numbers, what they usually search for, and more.

- **Trojans**: This type of malware masquerades as legal software or is hidden behind legal but corrupted software. It tends to act discreetly and creates backdoors on a person's security to let in other malware.

- **Botnets**: A network of infected computers that are under the control of a single main computer, all working together to accomplish a goal.

- **Adware**: While not always malicious in nature, this advertising software can greatly impair security, which can make it easier for other threats to enter.

- **DDoS**: Overloading a website or software with information that can give hackers a hint that can cause the site to become blocked and have to be shut down. It can be avoided with antivirus, firewalls and filters.

- **Phishing or Pharming**: Attempts to gain sensitive information that could lead to an intruder entering the network assuming identity of a legitimate source. Phishing is by email. Pharming is for fake websites and servers.

- **Ransomware**: It aims to hijack the computer by blocking its access to your machine's system and charging a ransom amount to free access.

- **Scareware**: Also known as cheating software, scareware may appear as legitimate notifications from antivirus companies, claiming that the computer has been infected and needs new software. However, by downloading the new program, personal information and passwords are stolen.

- **DNS Cache Poisoning**: It is the poisoning of the DNS protocol of the machine. This technique can be used to direct users from one site to another criminal, which may contain malicious content.

3 Cybersecurity care in educational institutions

Many institutions unfortunately feel that opting for information protection measures with new technologies and investing in the newest solutions on the market is better than lowering the costs of information technologies and not having consequences behind those costs [13]. What happens is, funding to fix an error caused by an attack or malware gets more expensive than a solution that allows prevention, maintenance and periodic updates. If we make a quick comparison between these two, it is better to have a system in place to protect the information and updates needed than to pay for a database that has been damaged due to an attack that could have been avoided if we were properly prepared.

Even if the institution has information security measures, it is not 100 percent secure due to a common factor, people. People are not perfect, so they can make mistakes at any time. But more importantly, they are behind security. To mitigate the risk of failures, vulnerabilities, risks of information loss, or misuse of sensitive information, security policies need to be implemented.

This information security policy should be adaptable to the organizational environment and the language used should be easy to understand for all hierarchical levels, from student to teacher. It is necessary to create a hierarchy for access to the information provided because there is data in the institutions that should not be seen by students or within the reach of teachers. There are also certificates that can be obtained by testing to show the quality standard or the safety standard, and this can be a very important aspect for the customer. For example, if one institution has no certificate and the other has some type of certificate or quality standard, it is obvious that the client will choose the most qualified and the one, that shows them, the most requirements for data protection.

Following are some tips on what you can do to try to reduce the risk of attacks and how to protect educational institutions [14]:

- **Educate teachers, students, and staff**: Defining and enforcing security policies is very important. This policy should include passwords, emails, internet, good use policies and other important variables. Depending on the technology and processes used, the goal is to define rules and procedures that all people in the institutions must follow while using the institution's Wi-Fi network and other devices. Once it has been defined and completed, the security policy should be published in various places, easily accessible areas of the institution and even shared on social networks as a way to reach everyone and with the goal of implementing the policy. as soon as possible. It is essential that staff and students always stay informed and perform monthly training to see if they can detect malicious emails and other threats.

- **Layer Security**: Schools, universities, and other educational institutions need to have an antivirus that can, learn, and update as new threats are found. It is important to create and implement security layers such as firewalls, filters, antimalware, system update applications, and create backups for strong defense against threats. This approach is a way to protect data and devices in ever-changing environments. If, for example, the antimalware system is compromised, there are additional layers to ensure the institution's information is secure and intact.

- **Keep software up to date**: Educational institutions use numerous servers and applications with vulnerabilities that allow hackers to gain easy access to the network. Keeping the system up to date can provide great protection for the institution.
- **Backing up data on the network**: If hackers gain control over sensitive information and threaten to encrypt or destroy it, a recovery and backup strategy is essential. Using automated backup and recovery software ensures data is kept safe and accessible from anywhere.
- **Monitor the network**: You can ensure visibility across the network. Being able to remotely locate vulnerabilities and correct them saves IT managers time and protects the network from costly and scale damage.
- **Beware of the websites you access and download**: Different types of malware can be found anywhere but, are more commonly found on sites that have little security. To reduce the risk of finding malware simply use sites with high security and reputation. Before downloading, always double check that the author is trustworthy and read the reviews and comments as the malware may be installing without us realizing it.

4 Origins and motivations

Educational institutions are one of the sectors most vulnerable to the risk of cyberattacks. In the first part of 2018, there was more than three billion compromised information overall, but only focusing on education, 9% of the cases belonged to this industry [15]. Because educational networks are home to the kind of information hackers want, and because the academic environment is often open, networks tend to be easier to penetrate and hackers have more than enough reason to attack institutions that are not ready [16]. Like other types of organizations, universities, schools, and other places of education contain extremely valuable data for hackers, such as citizen card information, credit card numbers, and even medical data from students, teachers, and staff. All information stored in an institution is not guaranteed to be secure if a cyberattack occurs. Many institutions let in any type of user (student, teacher, alumnus, partners, vendors) but this can lead to a risk that cannot be protected against connecting to the site by devices that do not have the necessary protection. Hacker’s motives for attacking the network can be money, which is a major factor, but it can also be for espionage, to gain access to credential or sensitive data without anyone being aware of it. One more reason for hacking is illegally search information that is extremely valuable and confidential. This information may have been provided by teachers for an important study or by a student and no outsider should be able to access this type of data, but this is a great motivation for the hacker.

One of the reasons why there is such a high vulnerability in educational institutions that the risk of cyberattacks is so significant is that there is a high exposure to external users. Information breaches can turn into serious issues such as identity theft, stalking and intellectual property violations. Several institutions have limited budgets for information technology infrastructures and teams. Universities and schools focus budgets on equipment needed for school and labs, for example, and not to protect the network from hackers because they store thousands of sensitive and extremely valuable data for them. Thousands of devices connect to the network of institutions and as technologies evolve, the protocols for their protection are becoming outdated. Attention must always be paid to updating the system and protocols, as well as always informing teachers, as they are easy targets for attacks. The large areas available and created for students and other members of an institution can be another target because anyone can easily access the network.

5 Conclusion

Human behavior is and will continue to be one of the reasons cybercrime happens, such as taking advantage of personal data to pretend to be someone with access to a major network, stealing bank accounts or even blackmail.
Unfortunately, despite existing precautions, it is highly likely that cyberattacks, due to their great diversity and evolution, will continue to be adversity in the future. Given that hackers fit into our society, they will be in constant progress, finding ways, even if institutions protect themselves properly, to corrupt the network even if they have obstacles.

During the development of this paper, the idea of prioritizing protection in educational institutions is extremely significant.
To enable the use of technology and innovation, educational institutions should take the necessary measures and implement strategies to protect themselves against potential cyberattacks. To reduce the likelihood of attacks on sensitive data stored in the institutions database, staff, students and teachers need to be properly trained against the type of threats and to be aware of all types of hazards that may be exposed.

Given all that has been developed during this research, I conclude that there are various types of threats as well as their solutions, but institutions still today do not give due value to cybersecurity which makes the risk of attacks is continually present.

References

1. Calegari, C. (2015). *Educação Lidera Ameaças a cibersegurança. Porque e como reagir?* Obtained from Grupo Binário: https://www.binarionet.com.br/blog/educacao-lidera-ameacas-a-ciberseguranca-por-que-e-como-reagir/ , last accessed: 2019/12/12
2. Regus. *Ameaças à Cibersegurança e a sua origem e risco.* (2016) Obtained from Work Portugal: https://www.regus.pt/work-portugal/cybersecurity-threats-where-do-they-come-from-and-whats-at-risk/ , last accessed: 2019/12/12
3. *Segurança da informação para instituições de Ensino: Qual a importância?* (2018) Obtained from AllEasy: https://www.alleasy.com.br/2018/01/10/seguranca-da-informacao-para-instituicoes-de-ensino/ , last accessed: 2019/12/12
4. Greenberg, A. (2019). *This Teen Hacker Found Bugs in School Software That Exposed Millions of Records*. Obtained from Wired: https://www.wired.com/story/teen-hacker-school-software-blackboard-follett/ , last accessed: 2019/12/11
5. Obtained from DEF CON (2019): https://www.defcon.org/ , last accessed: 2019/12/9
6. Obtained from Blackboard (2019): https://www.blackboard.com/ , last accessed: 2019/12/9
7. Obtained from Follett (2019): https://www.follett.com/ , last accessed: 2019/12/12
8. *The Education Sector And The Increasing Threat From Cybercrime*. (2019) Obtained from SentinelOne: https://www.sentinelone.com/blog/the-education-sector-and-the-increasing-threat-from-cybercrime/, last accessed: 2020/01/10
9. *Common Types of Cyberattacks in Education and What We Can Learn from Them*. (2017). Obtained from Fortinet: https://www.fortinet.com/blog/industry-trends/common-types-of-cyberattacks-in-education-and-what-we-can-learn-from-them.html , last accessed: 2019/12/11
10. Basic survey on Malware Analysis, Tools and Techniques Dolly Uppal, Vishakha Mehra and Vinod Verma: International Journal on Computational Sciences & Applications (IJCSA) Vol.4, No.1, February 2014, last accessed: 2019/12/11
11. A Dynamic Malware Analysis for Windows Platform - A Survey M. Asha Jerlin and C. Jayakumar: Indian Journal of Science and Technology, Vol 8(26), DOI: 10. 17485 /ijst/ 2015/ v8i26/81172, October 2015, last accessed: 2019/12/11
12. Grimes, R. A. (2019). *9 types of malware and how to recognize them*. Obtained from CSO: https://www.csoonline.com/article/2615925/security-your-quick-guide-to-malware-types.html , last accessed: 2019/12/11
13. *Cybersecurity tips for schools*. (2019). Obtained from Avast blog: https://blog.avast.com/pt-br/cybersecurity-tips-for-schools , last accessed: 2019/12/9
14. Fraser, J. (2018). *Ameaças Cibernéticas: Por que o Setor da Educação é tão Atrativo?* Obtained from Marsh: https://www.marsh.com/br/insights/risk-in-context/ameacas-ciberneticas--por-que-o-setor-da-educacao-e-tao-atrativo.html , last accessed: 2019/12/11
15. Breach Level Index H1 2018 Infographic. *The reality of data breaches.* (2018) Obtained from gemalto, a Thales company: https://safenet.gemalto.com/resources/data-protection/breach-level-index-2018-h1/ , last accessed:2020/01/11
16. *3 reasons higher education is a cyberattack favorite*. (2019) Obtained from onelogin: https://www.onelogin.com/resource-center/topics/3-reasons-higher-ed-cybercriminals , last accessed: 2019/12/12

10.11228/dpsc.02.01.004

Portugal Cyber threats Review:

Targeted Health Institution

David Pinto

Lusófona University of Porto, Portugal
davidpinto15@gmail.com

Abstract. Over the years, there has been a larger improvement of technology, being present on most of the organizations, whether governmental or private, and being one of the fundamental components of their proper functioning, meaning that nowadays, big and most of medium corporations cannot work unless they have access to their servers and internet, showing how dependent they are to technology and how much impact an attack can have on their infrastructure.

Healthcare is no exception, given that technology is used from triage of the patient to their discharge, being used to save patients data, which medicines have taken or should take, all the medical history. This way, by storing all this data on servers, by becoming "online", health Institutions become potentials victims to attacks.

Throughout the paper, it will be done a review about the threats and attacks to Institutions in Portugal, focusing especially on the health Institutions, giving a real example of such attacks, how it was dealt with and ways to prevent and/or reduce them.

Keywords: Cybersecurity, Portugal, Threats, Attacks, Vulnerabilities, Healthcare, Information, Technology

1 Introduction

Technology and internet had a great advance in the last decades, given that is has been almost 30 years since the first medical record system based on a computer was proposed [1], till that date it was done manually. This advancement didn't affect just the way data is stored, it was also created new machines with the goal of facilitate the doctors work and improve the well-being and health of the patients. This way, Health Institutions became a new place for hackers to take advantage of, by having all their work fused with technology they have enabled themselves to possible cyberattacks.

Given that all the data about the patients is stored on a server, rather than some folders on a locker, it's natural that whoever wants access to this information, whether to use it themselves or to sell it to some companies, is willing to attack those infrastructures that contains it in order to seize it. Beyond their data, some patients require machines or electronic supports that are essentials for their health and well-being, such as implantable medical devices (IMDs), for example pacemakers or implantable cardioverter-defibrillators, which are electronic devices designed to treat abnormal physiological conditions within the body, which can vary from hearth failure to diabetes to Parkinson's disease, these devices can also fell victims to the

10.11228/dpsc.02.01.005

same hackers than seek your information, and even though technical security mechanisms has begun being developed it is not hack proof. [2]

However, things could be done to prevent or hinder the attacks, if the attack is successful there are measures to be taken in order to contain the data loss of patients and these attacks have consequences and cause damage.

All these questions will be addressed throughout this paper which focus on the theme threats to cybersecurity in Portugal, with special emphasis on health institutions. In section 2 is covered attacks and threats, giving examples, their consequences and the damage caused. Section 3, will be talked about vulnerabilities in health institutions, then a sub-topic about a specific attack to health institutions around the world and how Portugal fought against it and towards the end it will cover how health institutions operate in Portugal. Finally, conclusions are drawn in section 4.

2 Cybersecurity Threats and Attacks

Throughout the years, cybersecurity has had several definitions [3], also being in constant evolution, according to the author [4] cybersecurity is the prevention to the damage caused by the unauthorized usage of electronic information and of communication systems and the respective information contained therein, aiming to secure the confidentiality, integrity, and availability, including, as well, actions to restore the electronic information and the communication systems in the case of a terrorist attack or natural disaster, this definition leads to another, cybercrime, which is any criminal activity that involves a computer, networked device or a network, according to the U.S. Department of Justice it is divided into three categories, being them, crimes in which the computing device is the target, suck as in order to gain network access, crimes in which the computer is used as a weapon, like launching a denial-of-service attack, and crimes in which the computer is sued as an accessory to a crime, which happens when we store illegal data on our computer. [5]

Threats to cybersecurity could be classified into 3 types, naturals, non-intentional and intentional. The Naturals are due to hurricanes, storms, earthquakes, basically everything that it is not human related; The Non-Intentional involves all types of accidents, like spilling water on the server room causing damage to the server itself or the bad protection of a certain equipment; lastly, the Intentional, this one is more serious, because it’s the result of malicious actions by people. This last type will be the one given more emphasis since it’s the only that is considered a threat and the one that can hurt the corporations the most [6][7]. It can be categorized, as explained in this table 1. [8]

Table 1. Categories of attacks

Category	Description	Sub-attacks
Malware	Malicious software used to launch specific attacks in the computer systems	Spyware, Ransomware, Backdoors.
Network attack	Active or passive monitoring of computer communications and network traffic	Phishing, Spoofing, Exploit.
Network intrusion attacks	Any unauthorized activity on the computer networks	Trojans, Worms.
Social engineering attacks	Using social media and phone calls, attackers apply human psychology trick to make users giving access to sensitive information	Phishing.
Cyber espionage	Snooping on confidential information of a user or organization without permission	Industrial, Economic, Corporate espionage.
Reconnaissance	By finding out weaknesses in the network systems and services, attacker gathers sensitive information about the network	Port scans, packet sniffers.
Network access attacks	By searching out malicious activities in the network authentication, FTP and web services, the intruder gets access to a network system to obtain confidential information	Eavesdropping, Denial of service, Identity spoofing.
Cyber terrorism	Use of internet for electronic terrorist activities like large-scale disruption of computer networks, high-profile national components, national critical infrastructures or important business operations	Sabotage, Website defacement and denial of service.
Cyber warfare	Major disruption to national critical and highly important infrastructures through malign use of digital information	Disruption of nation's public services, Financial Institutions.

Now that we know the categories, here are so examples of possible attacks their explanations and some measures to prevent each attack:

- Phishing attack: the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.
- Backdoor: a backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing unauthorized remote access

to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected.

- Botnet: a botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. This can be as mundane as keeping control of an Internet Relay Chat (IRC) channel, or it could be used to send spam email or participate in distributed denial-of-service attacks.
- Clickjacking: A Clickjacking is a technique where cross-domain attacks are perpetrated by hijacking user-initiated clicks to perform unintended actions.
- Cross-Site Scripting: This is a type of attack that is responsible for computer security vulnerability, by injecting malicious scripts into the friendly and trusted web sites, these vulnerabilities can be used by attackers to bypass access controls.
- Eavesdropping: In Eavesdropping the attackers listens to the system’s or network’s conversation without their knowledge and uses that conversation for another attacker or enemy of that organization.
- Spoofing: Spoofing is an attack in which the attacker or program acts as if they are the actual, legitimate user of that system or network, hiding their originality from the network and impersonating the system admin or victim.
- Denial of Service: This attack has the goal of denying the user of resources and shutdown the services of the system by overloading its resources like bandwidth, TCP connection buffers and application/service buffer. [9] [10] [11] [12]

Even though attacks can happen to any institution, there are some measures that can be taken in order to prevent some attacks, here are some examples.

- Denial of Service: Filtering, Blackholing, Scale up Bandwidth, Outsourcing, Firewall and antivirus and Email filters.
- Spoofing: Network segmentation & access control, Physical Security, Packet filtering, Avoid trust relationships, Use cryptographic network protocols.
- Backdoor: Formatting hard disk, Use of file scanner, Setup Firewall.
- Eavesdropping: Access Control, CCTV installation, Securing the Area, Awareness Training.
- Phishing: Anti-phishing toolbar, Blocking of Pop-up, Updating of browser, Secure links, Back-up of data.
- Cross Site Scripting: Data Validation, Data Sanitization, Output Escaping.
- Botnet: Change of Passwords, Encryption. Put IoT devices on a separate network, Keep Firmware Up-to-Date, Turn off Universal Plug-and-Play.
- Clickjacking: Install a Spam & Virus Firewall, Filter Web Traffic and Block Malicious Sites, Periodically Logout Users, Update Internet browser and plug-ins such as Flash. [11]

Profile of the attackers, students, just to have some fun snooping on people’s email, ex-employer, perhaps they were not too happy for being let go, so they decide to take revenge by attacking their former company, a sales representative, they do this so they can trick the other people into believing they are better than they really are or that they represent something/someone bigger/better than they actually do, a businessman, to discover a competitor’s strategic marketing plane, and finally a cracker, and in order to explain their motive we should explain who they are, although they can be compared to hackers, there are some differences, while hackers are normally seen as ethically correct, white hats that do their work in order to find loopholes and to restore the security of corrupted networks to build a secure system, and when they do it, it’s with the consent of their hiring organization, crackers do it for personal gain, usually hackers have the knowledge and skill to create their own programs, unlike the crackers which prefer to use software available to them, their goal is to break the security of someone’s computers and networks for the purpose of engaging in illegal activities. [7] [9] [10]

Table 2. Profile of attackers

Profile of attacker	Goal
Student	Have fun
Ex-employer	Revenge
Sales Representative	Trick people
Businessman	Discover competitor’s strategy
Cracker	Personal gain

3 Targeted Health Institutions

Health institutions are some of the organizations we have to trust the most, it´s them that hold a lot of our personal and private information such as, name, date and place of birth, medical record and social security number, while having several flaws, like low budget, lack of IT organization and excessive use of legacy systems, because of it, they become one of the best and most frequent targets for hackers.

In the last years, medical fields have grown in terms becoming more technology dependents, electronic health records (EHRs), which are the digital versions of a patient’s chart, have appeared, clinical systems have been automated, resulting in a evolved workflow that brings news and increased security challenges, the systems are interconnected and mobile devices are being used as remote accesses and data sharing, all these new aspects are in constant evolution, however, the cyber threats are also in constant evolution, hackers besides stealing the patient’s data, can they can alter any patient medical records, compromise medicine inventory systems or even cutting off power supply resulting in the unnecessary risk of the patient’s lives. [13]

Vulnerabilities are a key component on the impact hackers have since it makes their job easier. Vulnerability is a weakness that allows an attacker to compromise the availability, confidentiality or integrity of a computer system, these may be the result of a programming error, a flaw in the design or implementation or even a bad management which affects the security, it not only can affect software, but hardware as well. According to [14], the greatest vulnerabilities come from external attackers and sharing data with third-parties.[15] Attacks that focus on the network to penetrated the service usually aim at three targets, web servers, databases and application software. The weakness with using a web service is that this one normally contains vulnerabilities that can be easily exploited by the attackers with the number of tools available to them that can scan web interfaces and highlight those vulnerabilities; To store all the information about the patients, medical services use databases servers, which, if not configured correctly are vulnerable to SQL injection, with the SQL injection the attacker has power over all the three goals of information security, confidentiality, integrity and availability, they can see, delete, steal or change information; For those who use application software, this is, those who use any software running on any device, a rigorous software vulnerability teste should be done to it, otherwise error in the code could be a weakness exploited by attackers. [16]

3.1 WannaCry Ransomware attack

The WannaCry attact in May 2017 affected multiple types of organization around the whole world, making thousands of hostages, and health institutions were not excluded from this with an exception.

The WannaCry malware is a self-propagating ransomware that spreads through internal networks and over the public internet by exploiting vulnerability in Microsoft's Server Message Block (SMB) protocol. It consists of two distinct components, one that provides ransomware functionality and another used for propagation, which contains functionality to enable SMB exploitation capabilities. The malware appends encrypted data files with the .WCRY extension, drops and executes a decryptor tool, and demands an amount of money to decrypt the data. [17] Two days after the attacks have started to appear on several continents and organizations on 12 May 2017, SPMS (Shared Services of the Ministry of Health) issued a normative circular referring the same attack where the next protective measures were taken: The use of email was conditioned, only fax/phones were being used to communicate; Additional mechanisms of security were added to the use internet, these mechanisms could, in websites which held a reduced reputation, be conditioned; All the computers were to be shut down from the 14 to the 15 of May; On the 15 and 16 of May, the computers without internet connection should detect and report any anomalous situations to the computer services, the ones connected to the institution network would have to wait until the implementation of the recommended security measures; If any user detects any suspicious messages or change in the equipment operation, that person must unplug the computer down immediately, it must also report the situation to the computer services of that institution and the servicedesk of SPMS; All the suspicious email or file found on the pc must be reported to the computer services of that institution and the servicedesk of SPMS; If any worker from the National Health Service (SNS), Ministry of Health (MS) or any hospital had, in the distant or recent past, any situation with encrypted files and texts, with a ransom, that information should be immediately reported to the servicedesk of SPMS, informing the where, which and when it happened. [18] With this normative circular, the SPMS got ahead of the attack, and with it dodged being attacked like many other countries and institutions, from the 10 thousand machines infected with the WannaCry ransomware in Portugal, the institutions that answered to the SMPS were not infected. [19]

3.2 SPMS

On this sub-topic, a few questions were made to someone in the Ministry of Health Shared Systems (SPMS), regarding the operation of health institutions in Portugal such as prevention measures or measures taken after an attack, given that the SPMS oversees the health Institutions in Portugal and the answers will be talked about here.

Ministry of Health Shared Systems is a concept to which a majority of corporations resort, hiring specialized services with the purpose of decreasing fixed costs on some activities.

The SPMS, EPE, as one of the central entities in the Ministry of Health has as mission the provision of shared services in the following areas – purchasing and logistics, financial services, human resources and systems and technology of information and communication – to the entities with specific activity in the health area. Regarding cybersecurity the SPMS, EPE should articulate with the GNS/CNCS (National Security Office/National Cybersecurity Center) in order to promote the articulation intra-institutional and interinstitutional with a view to ensure the cybersecurity of health information networks and systems, regardless of your location, depending on existing connectivity, such as keep up with, support and monitor the protection measures, detect, respond and recuperation of critical resources of SNS (National Health Service-). Thus, being that most of public hospitals are a public business entity, with administrative, financial and patrimonial autonomy, the protection and prevention measures from each of the health institutions are managed and enforced internally, performing the measures referred in normative circulars of SPMS or centrally provided services. Giving an example, the following normative circular, nº 07/2017/SMPS: Infrastructure reinforcement measures and systems operation, which is divided into 5 categories, that informs the responsibilities of the entities regarding network infrastructure, systems infrastructure, datacenters and system rooms, technical skills, security and operation, the SPMS responsibilities, measures to have in contingency and crisis situations, informing institutions about the topics a contingency plan needs to have, the SPMS contact mechanisms, actions and information to be submitted and the need to perform simulations and recommendations.[20]

According to the dispatch n. º 1348/2017, it was established that the SNS entities and the MS services and organisms are required to notify security incidents to SPMS, EPE, through their Responsible Notification Officer (RNO). This mandatory centralized cybersecurity notification procedure (NOCICS), predict to categorize cyber security incidents according to 9 classes, in accordance with the taxonomy used by the National CSIRT Network and National Cybersecurity center (CNCS) and where justified, the incidents are reported to the CNCS. [21]

According to the SPMS, the most frequent attacks are related to phishing, malware and intrusion attempts by exploiting vulnerabilities, often stemming from legacy web portal that were not developed using security best practices. However, the attack surface amplitude is limited by the existence of RIS (Health Computer Network), which by default does not permit direct internet access.

4 Conclusion

With all the cybersecurity threats and attacks available, it's important, now more than ever to bet on a serious and sophisticated cybersecurity capable of protecting everybody's information, and also use the profile of attackers to determinate where and how they pretend to attack, so institutions can be prepared for it.

Even though by going offline, the health institutions in Portugal were able to not get infected by the malware, it should have not been their solution to the problem, by doing so they were showing how unprepared health institutes were in terms of cybersecurity in which a measure to stop the attack was shutting down everything from online.

With this work I've learned that for the number and importance of the information and lives health institutes are responsible for, their security should be better, just like the minds of the employees when it comes to opening suspicious emails or enter suspicious websites, however, the security has been improving over the years, showing that they realize the importance and want to keep it safer from every threat.

References

1. Scielo, http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1415-65552001000100007, last accessed 2019/11/25
2. Denning, T., Borning, A., Friedman, B., Gill, B., Kohno, T. & Maisel, W.: Patients, Pacemakers, and Implantable Defibrillator: Human Values and Security for Wireless Implantable Medical Devices, pp.1-2 (2010)
3. Nicole M Tucker, Cybersecurity: Deciding the Effectiveness of the U.S.Comprehensive Cybersecurity Initiative, pp.1-2 (2015)
4. Cavalcanti, C., "Cyberdefense: Challenges and comparative legislation between Brazil and Portugal", pp.3-6 (2017)
5. SearchSecurity, https://searchsecurity.techtarget.com/definition/cybercrime, last accessed 2019/12/02
6. Breda, F., Barbosa, H., Morais, T.: Social Engineering and Cyber Security, pp.1-5 (2017)
7. Barbosa, H., Magalhães, R.: Cyber Espionage and Digital Privacy, pp.1-3 (2017)
8. Prasad, R, Rohokale, V.: Cyber Security: The Lifeline of Information and Communication Technology. 1st edn. 2020 edition Springer, pp.16-30 (2019)
9. European Commission: Cyberroad- Development of the Cybercrime and Cyber-terrorism Research Roadmap, n. º 607642 , pp.10-11 (2015)
10. Securitytrails, https://securitytrails.com/blog/hacker-vs-cracker, last accessed 2019/12/06
11. Dutta, L., Sumi, F. H & Sarker, F.: A review on Cyberattacks and Their Preventive Measures. International Journal of Cyber Research and Education, 1(2), pp.14-25 (2019)
12. Jamwal, K & Sharma, L. S.: Clickjacking Attack: Hijacking User's Click. International Journal of Advanced networking and Applications, pp.1-2 (2018)

13. Le Bris, A. & El Asri, W.: State of Cybersecurity & Cyber Threats in Healthcare Organizations, pp.10 (2006)
14. KPMG, “Health care and cyber security: Increasing Threats Require Increased Capabilities”, pp.1-2, (2015)
15. Symantec: ISTR Healthcare, vol.22, (2017).
16. Williams, P. & Woodward, A.: Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Medical Devices: Evidence and Research, pp.309 (2015)
17. Kumar, M.S., Ben-Othman, J. & Srinivasagan, K.G.: An Investigation on Wannacry ransomware and its Detection, pp.1-2 (2018)
18. Circular Normativa nº01, Medidas excepcionais ciber-segurança: http://spms.min-saude.pt/wp-content/uploads/2017/05/Circular-Normativa-n%C2%BA1-SPMS-medidas-ciber-seguran%C3%A7a-v.2.pdf, (2017), last accessed 17/12/2019
19. exameinformatica, http://exameinformatica.sapo.pt/noticias/internet/2017-05-15-WannaCry-12-mil-computadores-infetados-em-Portugal, last accessed 16/12/2019
20. Circular Normativa n.º 07/2017/SPMS, Medidas de reforço de infraestruturas e operação de sistemas: https://spms.min-saude.pt/wp-content/uploads/2017/09/Circular_Normativa-N.07_2017.pdf, (2017), last accessed 20/12/2019
21. Despacho n. º 1348/2017, Diário da República n. º 28/2017, Série 2 de 2017-02-08, https://dre.pt/home/-/dre/106415139/details/2/maximized?serie=II&dreId=106415113, (2017), last accessed 20/12/2019

Information Privacy and Security on a Shared Resources Network: IP Spoofing Attacks

Pedro Graça[1]

[1] Lusofona University of Porto, Portugal
a21705454@mso365.ulp.pt

Abstract. In today's age, people consume and share information at an enormous rate. We live in a world where information is power and more importantly, money, lots of it. Companies are now increasingly requesting more sensitive information from their users, in order to provide better services to its customers. This paper focuses on underlining the importance of information privacy and security on a shared resources network, by analyzing the current level of awareness of the general population and of some of the most important governments around the world to such matters, discussing how the "benefits of the internet" and privacy issues are intertwined with each other, ways to achieve a good level of privacy and security while maintaining the same usability and comfort that people have grown accustomed to, explain how one's data can be important to many different entities such as companies and their advertising partners but also to ill-intentioned individuals wanting to profit from it or just intending to cause grief to others. The last section of this paper lists and describes the major threats to digital privacy and security, with special emphasis in one type of threat: IP Spoofing Attacks.

Keywords: Data, Confidentiality, Shared Resources Network, Privacy, Threats, Security, Availability, IP Spoofing.

1 Introduction

In the last decade, the bond between humanity and technology has only grown stronger. Our dependency on technology increases every year, as well as the benefits we get from it such as: the ability to talk to our friends, colleagues, family even a complete stranger, without any tariffs attached to it as long as we have an internet connection, the capacity of being able to acquire knowledge about any topic just by using a search engine and also, being able to share a photo or video with whoever we want whenever we want, instantaneously.

Despite the countless benefits technology brought us, it also brought us new dangers and ways of making us vulnerable to other entities, and these threats and vulnerabilities are increasing every year, as time passes by. [1]

Each time a person posts or shares an image, accesses a website, watches a video or buys something online, they leave behind a "digital trail" of themselves which can be used to analyze, track and identify an individual.

10.11228/dpsc.02.01.006

This "digital trace" is more commonly known as "digital footprint" [2], and unlike the snow or dirt footprints we see in real life, this type of trail cannot be erased just by simply throwing a dirt or snow on top of it. In fact, each footprint we leave behind in our "digital journey" is permanent, and some people are already realizing this when they are suddenly fired from their current job due to some tweet they wrote years ago, which was the case of James Gunn [3], a writer/director who worked for Disney and saw himself fired because of a series of tweets he wrote, some a decade old.

Section 2 of this paper talks about how important it is for people to be aware of the dangers of the internet and be more careful about what they share on places like social media, but also raise their awareness about how valuable their own data can be when it is available to everyone on the internet. Besides regular people, this section also emphasis the importance of the government on this matter, and how it should protect its citizens against evil entities and non-privacy respecting companies.

Section 3 shows how privacy and the internet are strongly connected, the various threats that exist and simple steps that help counter them, or at least diminishing the chances of being affected by one.

Section 4 presents a review of IP Spoofing attacks, the various forms an attack of this kind can take, an example of how one is performed and what results come from the success of one.

2 Social and Governmental Awareness on Online Privacy and Security

With how much impact the internet can have in everyone's life, we will now explore the current level of awareness, both social and governmental, on this subject and try to understand how governments are dealing with these digital threats, what measures are being taken to solve them or at least trying to diminishing them as much as possible and also, how much do ordinary people care about the safety and privacy of their digital information, what kind of precautions do they take when they access the internet, or if they just live their lives defenseless against any evil entity, hoping they never become victim of a cybercrime.

2.1 Social Awareness

An article published last year by the South African Journal of Science [4] analyzes and describes the importance of information privacy and online security by conducting a study using Facebook as the study's test environment, to evaluate how much of their personal lives people share on Facebook, and the results do not look good.

From a population of 357 users, the study found that 67% (n = 240) of Facebook users' personal data are partially available, while the remaining 33% (n = 117) have all of their personal details available to anyone (See figure 1).

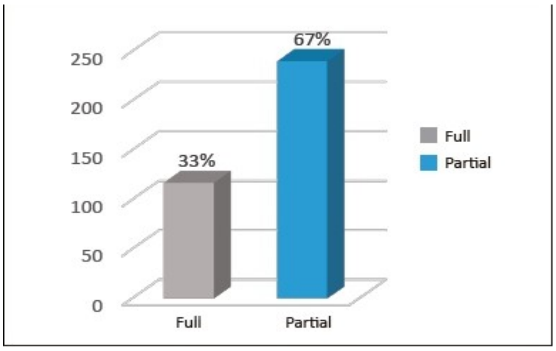
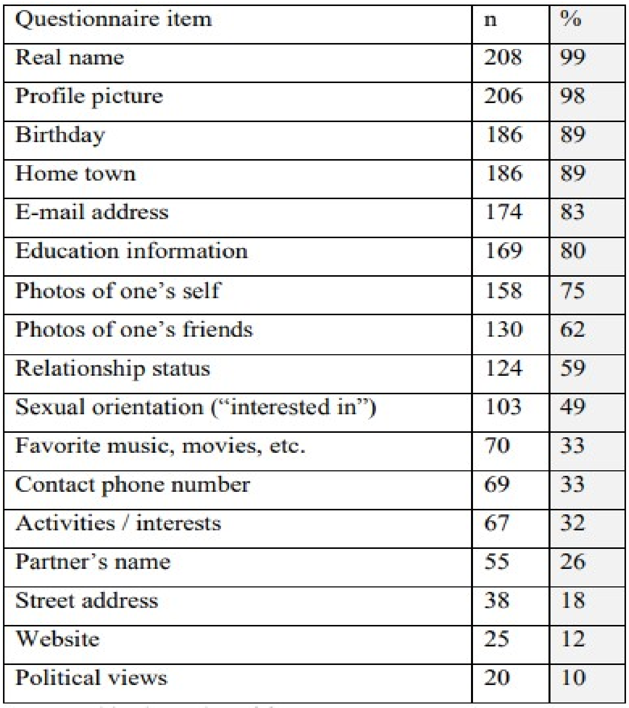


Fig. 1. Availability of users' data [4]

Another study, which also targets Facebook as their case study, wrote a paper in which it says that of the 210 respondents who participated in the study, only 2 of the 210 informed that they did not appear with their real names on Facebook [5]. Besides the astounding percentage of people who disclose their real name on Facebook (99%), the study dug deeper in what kind of information users share willingly on the social network and the results look very dim when it comes to privacy concerns.



Questionnaire item	n	%
Real name	208	99
Profile picture	206	98
Birthday	186	89
Home town	186	89
E-mail address	174	83
Education information	169	80
Photos of one's self	158	75
Photos of one's friends	130	62
Relationship status	124	59
Sexual orientation ("interested in")	103	49
Favorite music, movies, etc.	70	33
Contact phone number	69	33
Activities / interests	67	32
Partner's name	55	26
Street address	38	18
Website	25	12
Political views	20	10

Fig. 2. Personal information on profile [5]

Analyzing the table above, we can conclude that most respondents share a lot of their personal information on Facebook, making the process of gathering personal details of an individual, a simple and quick task for any interested party.

2.2 Government's Role

Despite information privacy and security being something that should be achieved mostly by each one of us, there are some things the average person can't control and should be taken care of by the government. For example, the situation of good companies becoming evil or too big, that they start thinking they can get away with anything, prevent data breaches, data mining and also the case of the government itself that should not abuse of the power it was bestowed with, as it is seen in some totalitarian countries [6], who use their powers to spy on their own citizens and citizens of other countries as well.

There's also a serious matter these entities should be paying attention to, and that is cybercrimes. There are many types of cybercrimes, and although some can be prevented by users, some can only be stopped and prevented by companies or governments.

Phishing emails, DoS attacks and Identity theft, are only a few types of cybercrimes [7] that can occur and should be fought against, now more than ever.

According to a news article [8], cybercrime is the fastest growing type of a crime in the U.S, and they are increasing in size, sophistication and cost. It is estimated that cybercrimes will cost $6 trillion annually by 2021, up from $3 trillion in 2015 [8].

After analyzing this data, it is evident that this is a problem that cannot be ignored either by us ordinary people or by governments, and should be payed attention to, before something serious happens, something that could be prevented if we had put a bit more effort in trying to comprehend and understand how this "digital world" works when there was still time to act.

3 Internet Benefits and How it Affects Privacy and Security

The internet today allows us to do many things, that we couldn't fully explore it in a single lifetime (Watching all YouTube videos would take more than that).

A few decades ago, if someone didn't know something about a specific theme, that person would have to go to a library and read a book about it or ask someone specialized in that specific area to explain it to them, but today you just insert your question on any available search engine and within a few seconds (or less), you have all kinds of information about the subject you were curious about, and all of this is available through a computer or a cellphone, millions and millions of documents, articles, news, all of it in the palm of your hand [9].

Amazon for example, allows us to read and choose from an enormous collection of online books, but this come with the cost of a portion of our online privacy, since amazon, as well as other companies, can track where someone started reading something, what was read/reread, what passages were marked or even if you finished reading that particular book. [10]

Additionally, if you open any social media website, you're flooded with all kinds of information: pictures and videos of your friends, "internet memes", news, there's just no end in sight.

These are only a few of the many things we can do by using the internet, but as mentioned before, every page you visit and all the "likes" you put on Facebook, are being tracked and not by the entities people commonly think about. It has become a norm, that every webpage we visit has some kind of advertising, and a large portion of these advertisement uses ads that have a strong possibility of being relevant to you [11]. This is what's called "targeted advertising" and although it can be beneficial to us, it comes with a cost, and that cost is our online privacy.

In order for "targeted advertising" to work, websites and companies have to collect has much data as they can about each one of us, in order to provide ads about things we like and might be interested in buying. This brings up the question of "how much can we trust in these companies" and "what do they do with their consumers personal information", we can only speculate, and so is up to governments to take a step forward and regulate what is allowed and not allowed to do done with our data.

Taking the United States as an example, there are virtually no government regulations on privacy policies and disclosure in e-commerce or on the Internet [12], this meaning that we are all at the mercy of a company's good will, and our data can be used in anyway they see fit.

3.1 Threats to Our Digital Privacy and Security

Unfortunately, the number of threats that exist nowadays is vast and is constantly increasing and stating and describing every one of them would lead to a whole other paper. Therefore, in this section, there are only going to be mentioned some of the most important threats that can affect network traffic, such as malwares.

Security Objectives

The classic model for information security defines three objectives of security: maintaining confidentiality, integrity, and availability [13].

- Confidentiality refers to protecting information from being accessed by unauthorized parties.
- Integrity focuses on ensuring the authenticity of information (that information is not altered, and that the source of the information is genuine).
- Lastly, availability means that information is accessible by authorized users.

List of Existing Threats

- Malware
- Phishing
- Trojans

- Ransomware
- The list goes on

In the case of Malwares, they are developed by cybercriminals and can be installed on all sorts of devices and operating systems, and this type of attack is increasing at a fast rate, growing by a third in 2018 when compared to the previous year. [14]

With so many threats, each of them growing in number and sophistication, its vital users protect themselves in every way they can.

3.2 How to Protect Ourselves

This section lists things we can do in order to enhance the level of privacy and security of our digital information and to reduce our "digital footprint" as much as possible. [15]

As discussed, there are things that affect our information security and privacy that we can't really control, but on the scope of things we can control, here are some small steps that can have a big impact on the process of hardening the privacy and security of our online data:

- Use of long passwords with strong encryption
- Use of password managers
- Enable automatic updates
- Avoid giving crucial information when signing up on a website (e.g. real name, address…)
- Avoid accessing websites that hold crucial data about you (such as banks) on a public network
- Always log out of your accounts on a public computer
- Deletion of "cookies" to reduce the risk of cross-website tracking
- For additional security, connect to websites which use encrypted DNS and HTTPS

These simple steps can greatly reduce the amount of information a person leaves behind when browsing the internet, either to evil individuals, advertising companies, a person's ISP (Internet Service Provider) or even governments in the most extreme cases. [16]

4 IP Spoofing Attacks

The last section talked about some types of attacks that we can be a target of, ways to reduce our digital footprint, and reduce the chances of having our digital information stolen or compromised.

This section will focus on a specific type of attack: IP Spoofing attacks, what they are, types of IP Spoofing, how to perform one, conducting an actual IP Spoofing attack. Lastly, we'll analyze the data obtained from the attack, with the aim of widening our knowledge about this subject.

4.1 Definition and Existing Types of IP Spoofing

Before diving into the actual testing and experimenting, let's first understand some key concepts about IP Spoofing attacks. To put it mildly, an IP spoofing attack is the creation of Internet Protocol (IP) packets which have a modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both. [17]

From a legal perspective, IP Spoofing is not a criminal activity since the act in itself (of spoofing an identity) is not illegal. It only becomes illegal when a threat of death or violence is involved, or personal data are stolen in order to commit fraud or identity theft. [18]

There are various types of IP Spoofing attacks namely "Distributed Denial of Service" more commonly known as DDoS, "Blind Spoofing", "Non-blind Spoofing", "Man in the Middle Attack", the list goes on.

4.2 Methodology and Testing

In this section, an IP Spoofing attack will be conducted between two machines, so that we can see how a typical IP Spoofing attack works and what kind of damage it can cause. Note that the attack was merely done for academic purposes and is done in a controlled environment, meaning that no entity or individual will be harmed.

Hardware and Software Used

- 1 machine with Windows 10 installed (The attacker)
- 1 machine with Linux installed (The target/victim)
- Wireshark - "Wireshark is the world's foremost and widely-used network protocol analyzer." [19]
- Colasoft Packet Builder – Enables the creation of custom network packets [20]

The Colasoft packet builder allows an entity to send ICMP (ICMP or "Internet Control Message Protocol", is a software component of the Internetworking layer of TCP/IP; essentially, it is a companion at that level to IP itself [21]) request with a spoofed IP address, create custom network packets (Custom TCP or UDP packets) and send them over a network as a valid request.

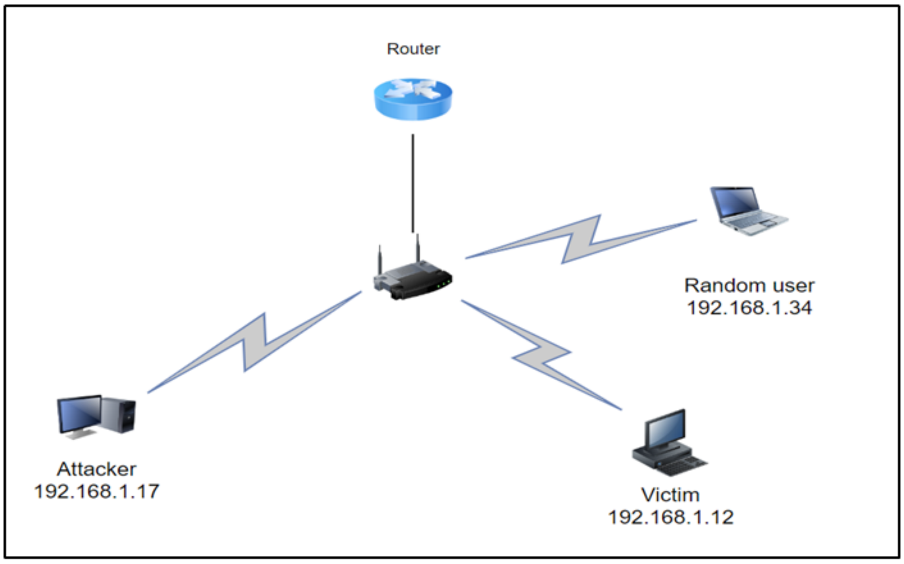


Fig. 3. Network constitution

Overview

As we can see, there are three hosts: the attacker, the host we want to target and a random authorized user in the network.

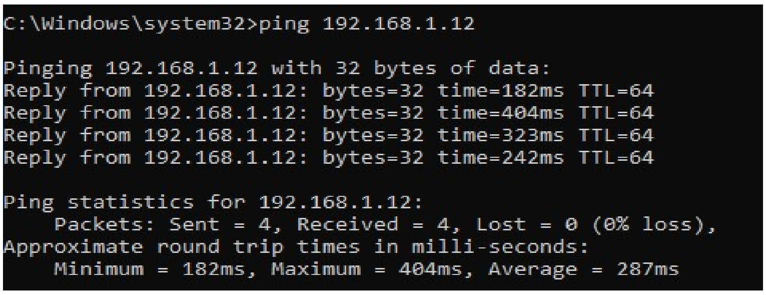
The test will consist in capturing ICMP packets that are heading towards the target machine (the machine with the IP address 192.168.1.12).

After grabbing the ICMP packets, we will modify the packet's source IP address by replacing it with a different IP address, for example with the random user's IP address (192.168.1.34). Lastly, we will verify if the target receives ICMP requests with the spoofed IP address.

Testing

To start the test, we must initialize "Wireshark" in order to start capturing packets.

Through the windows command line on the attacker machine, we will ping the victims IP address with 32 bytes of data.

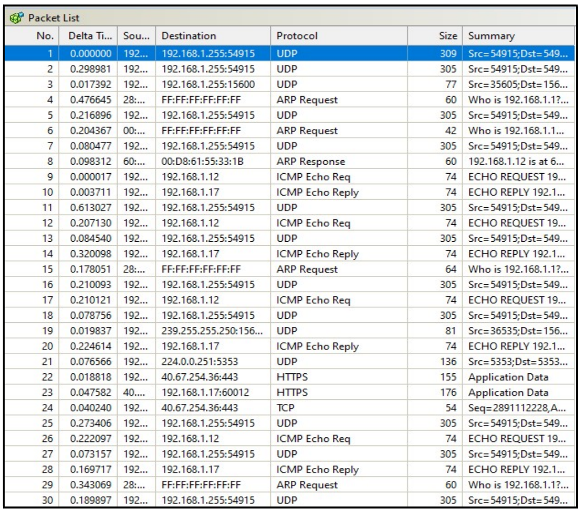


```
C:\Windows\system32>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:
Reply from 192.168.1.12: bytes=32 time=182ms TTL=64
Reply from 192.168.1.12: bytes=32 time=404ms TTL=64
Reply from 192.168.1.12: bytes=32 time=323ms TTL=64
Reply from 192.168.1.12: bytes=32 time=242ms TTL=64

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 182ms, Maximum = 404ms, Average = 287ms
```

Fig. 4. Sending pings to target host

Now with the Wireshark software we will save the captured packets to a file, so we can modify them with the “Colasoft Packet Builder” software.

Loading the Captured Packets



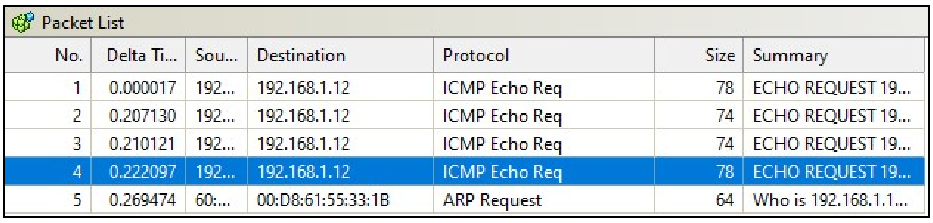
Packet List

No.	Delta Ti...	Sou...	Destination	Protocol	Size	Summary
1	0.000000	192...	192.168.1.255:54915	UDP	309	Src=54915;Dst=549...
2	0.298981	192...	192.168.1.255:54915	UDP	305	Src=54915;Dst=549...
3	0.017392	192...	192.168.1.255:15600	UDP	77	Src=35605;Dst=156...
4	0.476645	28:...	FF:FF:FF:FF:FF:FF	ARP Request	60	Who is 192.168.1.1?...
5	0.216896	192...	192.168.1.255:54915	UDP	305	Src=54915;Dst=549...
6	0.204367	00:...	FF:FF:FF:FF:FF:FF	ARP Request	42	Who is 192.168.1.1...
7	0.080477	192...	192.168.1.255:54915	UDP	305	Src=54915;Dst=549...
8	0.098312	60:...	00:D8:61:55:33:1B	ARP Response	60	192.168.1.12 is at 6...
9	0.000017	192...	192.168.1.12	ICMP Echo Req	74	ECHO REQUEST 19...
10	0.003711	192...	192.168.1.17	ICMP Echo Reply	74	ECHO REPLY 192.1...
11	0.613027	192...	192.168.1.255:54915	UDP	305	Src=54915;Dst=549...
12	0.207130	192...	192.168.1.12	ICMP Echo Req	74	ECHO REQUEST 19...
13	0.084540	192...	192.168.1.255:54915	UDP	305	Src=54915;Dst=549...
14	0.320098	192...	192.168.1.17	ICMP Echo Reply	74	ECHO REPLY 192.1...
15	0.178051	28:...	FF:FF:FF:FF:FF:FF	ARP Request	64	Who is 192.168.1.1?...
16	0.210093	192...	192.168.1.255:54915	UDP	305	Src=54915;Dst=549...
17	0.210121	192...	192.168.1.12	ICMP Echo Req	74	ECHO REQUEST 19...
18	0.078756	192...	192.168.1.255:54915	UDP	305	Src=54915;Dst=549...
19	0.019837	192...	239.255.255.250:156...	UDP	81	Src=36535;Dst=156...
20	0.224614	192...	192.168.1.17	ICMP Echo Reply	74	ECHO REPLY 192.1...
21	0.076566	192...	224.0.0.251:5353	UDP	136	Src=5353;Dst=5353...
22	0.018818	192...	40.67.254.36:443	HTTPS	155	Application Data
23	0.047582	40....	192.168.1.17:60012	HTTPS	176	Application Data
24	0.040240	192...	40.67.254.36:443	TCP	54	Seq=2891112228,A...
25	0.273406	192...	192.168.1.255:54915	UDP	305	Src=54915;Dst=549...
26	0.222097	192...	192.168.1.12	ICMP Echo Req	74	ECHO REQUEST 19...
27	0.073157	192...	192.168.1.255:54915	UDP	305	Src=54915;Dst=549...
28	0.169717	192...	192.168.1.17	ICMP Echo Reply	74	ECHO REPLY 192.1...
29	0.343069	28:...	FF:FF:FF:FF:FF:FF	ARP Request	60	Who is 192.168.1.1?...
30	0.189897	192...	192.168.1.255:54915	UDP	305	Src=54915;Dst=549...

Fig. 5. List of captured packets

From the image above, we can see that there is a lot of data, but the data that interests us is the one where the protocols are labeled “ICMP Echo Req” and “ARP Request”, hence we will remove everything else that falls out of this spectrum.

Removing Unnecessary Data



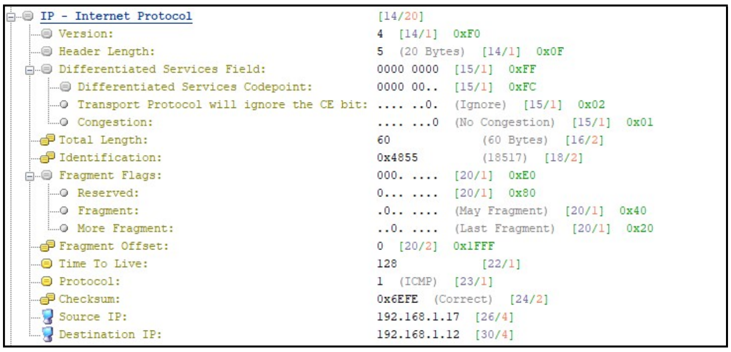
Packet List

No.	Delta Ti...	Sou...	Destination	Protocol	Size	Summary
1	0.000017	192...	192.168.1.12	ICMP Echo Req	78	ECHO REQUEST 19...
2	0.207130	192...	192.168.1.12	ICMP Echo Req	74	ECHO REQUEST 19...
3	0.210121	192...	192.168.1.12	ICMP Echo Req	74	ECHO REQUEST 19...
4	0.222097	192...	192.168.1.12	ICMP Echo Req	78	ECHO REQUEST 19...
5	0.269474	60:...	00:D8:61:55:33:1B	ARP Request	64	Who is 192.168.1.1...

Fig. 6. Filtered captured packets list

After removing the unnecessary data, we are left with only five packets (we are only going to need one of the ARP Request so no point in keeping more than one).

Each packet has a set of parameters we can edit using the “Colasoft Packet Builder” but for this test, we are only going to edit the field called “Source IP”.



```
IP - Internet Protocol                              [14/20]
  Version:                                          4  [14/1]  0xF0
  Header Length:                                    5  (20 Bytes)  [14/1]  0x0F
  Differentiated Services Field:                    0000 0000  [15/1]  0xFF
    Differentiated Services Codepoint:              0000 00..  [15/1]  0xFC
    Transport Protocol will ignore the CE bit:      .... ..0.  (Ignore)  [15/1]  0x02
    Congestion:                                     .... ...0  (No Congestion)  [15/1]  0x01
  Total Length:                                     60             (60 Bytes)  [16/2]
  Identification:                                   0x4855         (18517)  [18/2]
  Fragment Flags:                                   000. ....  [20/1]  0xE0
    Reserved:                                       0... ....  [20/1]  0x80
    Fragment:                                       .0.. ....  (May Fragment)  [20/1]  0x40
    More Fragment:                                  ..0. ....  (Last Fragment)  [20/1]  0x20
  Fragment Offset:                                  0  [20/2]  0x1FFF
  Time To Live:                                     128            [22/1]
  Protocol:                                         1  (ICMP)  [23/1]
  Checksum:                                         0x6EFE  (Correct)  [24/2]
  Source IP:                                        192.168.1.17  [26/4]
  Destination IP:                                   192.168.1.12  [30/4]
```

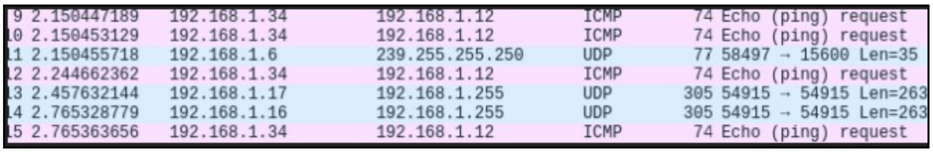
Fig. 7. Packet details

The "Source IP" field has the IP address of 192.168.1.17 (The IP address of the attacker machine). What we're going to do is change this value to 192.168.1.34 (The same IP address of the "Random user" described earlier) in all the packets we captured. After that's done, the last step is to send all the modified packets to the target host and analyze the results.

4.3 Results

To analyze the results, we're going to open "Wireshark" on the target machine and start capturing packets, to see if one host replies to another with a spoofed IP address.

After sending all the modified packets, we can stop capturing incoming packets on the target machine and review the results.



```
 9 2.150447189   192.168.1.34     192.168.1.12      ICMP     74 Echo (ping) request
10 2.150453129   192.168.1.34     192.168.1.12      ICMP     74 Echo (ping) request
11 2.150455718   192.168.1.6      239.255.255.250   UDP      77 58497 → 15600 Len=35
12 2.244662362   192.168.1.34     192.168.1.12      ICMP     74 Echo (ping) request
13 2.457632144   192.168.1.17     192.168.1.255     UDP     305 54915 → 54915 Len=263
14 2.765328779   192.168.1.16     192.168.1.255     UDP     305 54915 → 54915 Len=263
15 2.765363656   192.168.1.34     192.168.1.12      ICMP     74 Echo (ping) request
```

Fig. 8. Captured packets on the target host

As we can see, the host is replying to the other host with the IP address 192.168.1.34, making it look like it's the random user in the network that is interacting with the victim's machine, when in reality, the packets are being generated from the IP address 192.168.1.17 (The attacker's machine).

This is a simple test and is meant to show how IP Spoofing can be done.

In a similar way, attackers can spoof custom packets to obtain information from the target host or target network. This shows how important it is for people and organizations to protect themselves, implementing security measures to counter these attacks and prevent bad situations from happening.

5 Conclusion

This paper was written with the objective of enlightening and raising the awareness to how important information has become in this technological age.

The paper covered many different subjects, all of them related to information privacy and security on a shared resources network, ranging from social and governmental awareness to threats and invasion of our digital privacy, what type of enemies and dangers we face and how we can protect ourselves against them, and lastly, an analysis of the matter of IP spoofing attacks.

The subject of social and governmental awareness is serious, and we can conclude from the data presented in this paper, that it still has a long way to go until we can say both users and governments, are taking all the necessary measures to protect themselves or their citizens against the many digital threats.

Consequently, the paper also covered the existing threats to information privacy and security, as well as measures to counter them in order to leave no stones unturned.

For the last section, the matter of IP Spoofing attack was heavily covered, giving a brief explanation of the concepts involved, types of IP Spoofing and also, an exploration of the process carried out in the execution of an actual IP Spoofing attack and what damage can be done if an attack of this sort is successful.

References

1. Shu, Q., Tu, Q., & Wang, K. The Impact of Computer Self-Efficacy and Technology Dependence on Computer-Related Technostress: A Social Cognitive Theory Perspective. International Journal of Human-Computer Interaction, 27(10),) 923–939 (2011)
2. Jessica Ching, Why does your digital footprint matter?; https://www.giveagradago.com/news/2018/01/why-does-your-digital-footprint-matter/261, consulted on 19-11-2019
3. Bryan Bishop, “Writer-director James Gunn fired from Guardians of the Galaxy Vol. 3 over offensive tweets”; https://www.theverge.com/2018/7/20/17596452/guardians-of-the-galaxy-marvel-james-gunn-fired-pedophile-tweets-mike-cernovich, consulted on 19-11-2019
4. South African Journal of Science, “Privacy and user awareness on Facebook” ISSN 1996-7489; S. Afr. j. sci. vol.114 n.5-6 Pretoria May./Jun. 2018
5. Tuunainen, Virpi Kristiina; Pitkänen, Olli; and Hovi, Marjaana, "Users’ Awareness of Privacy on Online Social Networking Sites – Case Facebook" (2009). BLED 2009 Proceedings. 42. Article title. Journal 2(5), 99–110 (2016).
6. DigitalPrivacyWise, “Security is everyone’s responsibility, Privacy is yours.” https://medium.com/digitalprivacywise/security-is-everyones-responsibility-privacy-is-yours-7a4e46398db7, consulted on 22-11-2019
7. Panda Security, “Types of Cybercrime” https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime/ , August 2018, consulted on 23-11-2019
8. PR Newswire, “Cyberattacks are the fastest growing crime and predicted to cost the world $6 trillion annually by 2021”, https://www.prnewswire.com/news-releases/cyberattacks-

are-the-fastest-growing-crime-and-predicted-to-cost-the-world-6-trillion-annually-by-2021-300765090.html, December 18, 2018, consulted on 23-11-2019

9. Tijssen, R. J.Science dependence of technologies: evidence from inventions and their inventors. Research Policy, 31(4), 509–526 (2002)
10. Landau, S. Control use of data to protect privacy. Science, 347(6221), 504–506. (2015)
11. Roosendaal, A. Facebook Tracks and Traces Everyone: Like This! SSRN Electronic Journal. (2015).
12. Norman E. Bowie and Karim Jamal. Privacy Rights on the Internet: SelfRegulation or Government Regulation?. Business Ethics Quarterly, 16, pp 323-342 (2006)
13. "Information Security Basics", MDN web docs, https://developer.mozilla.org/en-US/docs/Web/Security/Information_Security_Basics/Confidentiality,_Integrity,_and_Availability, consulted on 28-11-2019
14. Jang-Jaccard, J., & Nepal, S. A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), pp 973–993 (2014)
15. Reeder, R. W., Ion, I., & Consolvo, S. 152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users. IEEE Security & Privacy, 15(5), pp 55–64 (2017)
16. Bellare, M., Paterson, K. G., & Rogaway, P. Security of Symmetric Encryption against Mass Surveillance. Lecture Notes in Computer Science, pp 1–19 (2014)
17. Cloudflare, "IP Spoofing", https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/, consulted on 03-12-2019
18. Vlajic, N., Chowdhury, M., & Litoiu, M, IP Spoofing In and Out of the Public Cloud: From Policy to Practice. Computers, 8(4), pp 81 (2019)
19. Wireshark, "Wireshark User's Guide"; https://www.wireshark.org/docs/wsug_html_chunked/Preface.html, consulted on 08-12-2019
20. Colasoft, "Colasoft Packet Builder", https://www.colasoft.com/packet_builder/, consulted on 08-12-2019
21. George Mays, Global Knowledge Course Director, CCISP, CCNA, A+, Network+, Security+, I-Net+, "How Does Ping Really Work?", Galaxy Visions, (2006)
22. Breda F., Barbosa H., Morais T., Social engineering and cyber security, (2017)
23. Magalhães R., Barbosa H., International Journal of Scientific & Engineering Research, Cyber Espionage and Digital Privacy, Volume 8, Issue 1, pp 396 (2017)

SESSION 2

Digital Contents Challenges in the Era of Digital

Analysis of Security in E-Commerce and M-Commerce
Nuno Mata

Major Challenges in Digital Contents Copyright Protection
André Fontes

Major Challenges in Digital Contents Copyright Protection
João Barreira

A Survey of Android Attacks Detection Techniques
José Duarte

Android Attacks Detection Techniques
Hugo Marques

Analysis of Security in E-Commerce and M-Commerce

Nuno Dias Mata
R. de Augusto Rosa 24, 4000-098 Porto, Portugal (2020)
Lusófona University of Porto
nunodmata@gmail.com

Abstract. This study explores the security related with E-Commerce and M-Commerce. With focus on the evolution and development of techniques that positively impact our safety using these services such as two factor authentication and strong database encryption we will understand how much it has changed. In contrast the consequent rise of more creative and different methods to breach these Websites or trick users into giving their personal data will be shown through examples like phishing sites, malicious links, key loggers, and further discuss what specific measures have been implemented to fight them. Nowadays the amount of traffic that visits these markets has increased exponentially which is correlated with the number of Websites and Apps developed throughout the last decade. It's clear why there is a necessity for continuous improvements in security for such fields, not only because the existing growth of the market but also given how sensitive the user submitted data can be.

Keywords: E-Commerce, M-Commerce, Authentication, Encryption, Phishing, Key Loggers

1 Introduction

With technology moving at high-speed no company can ever claim to be 100% covered by any security measure, even the slightest change to an IT system can make its security out-of-date. What needs to be addressed is the effect it would have on a business if all a company's data were to be destroyed, trading lines were brought down for a couple of hours (or worse a couple of days), or its home page was defaced. Not only would loss be measured in financial terms, but also in that of corporate image, leading to potential loss of customers and their confidence.

According to available data, online purchases have been steadily increasing since 2014 and e-retail revenues are projected to pass the 4 trillion US dollars in 2020 [1], and further studies show that 60% of Europeans (aged from 16 to 74) shopped online in 2019 [2].

Which means a wide variety of commerce is conducted via Electronic commerce (E-commerce) and the same can be said for Mobile-commerce (M-commerce), including electronic money transfer, supply chain management, online marketing, online transaction processing, electronic data interchange (EDI), inventory management systems etc. And is now being used in all types of business, including manufacturing companies,

10.11228/dpsc.02.01.007

retail stores, and service firms. It has made business processes more reliable and eminent. Consequently, E-commerce is now essential for businesses to be able to compete in the global marketplace today, and so maintaining these service's integrity is key, which means privacy and security are a major concern if companies want to keep consumers using the Electronic and Mobile markets. And it is known that many security issues are increasing day by day on the open internet like unauthorized access, client information leakage, credit card clowning etc [3].

The future is likely to be more alarming in the sense that crimes will be emitted without the knowledge and cooperation of the victim. Preventing cybercrime in the future will require strong E-security rather than plain human prudence. And that places most of the responsibility on developers, even though it's not possible to design a breach proof platform, their job is to make it as safe as can be, which also includes implementing visual clues and design details that lead users to make less errors. Which ideally would translate to not leaking and giving out involuntarily private information.

When it comes to mobile commerce, one of the main and important steps for gaining customer trust and attracting them is providing trust in mobile software and websites for making transactions. Trust over the mobile platforms is more critical due to the open nature of wireless networks. This was a challenge among researchers to conduct models, framework and studies about mobile commerce, trust in mobile commerce and customer issues in this type of business technology. Many studies highlight that an electronic commerce website with a greater level of trust usually gains tractions with a higher retention rate of consumer and higher degree of purchase intentions, and it is only natural.

Providing initial trust in well-designed websites leads to gaining trust from mobile customers. A variety of mobile topics in prior studies have been examined that include the impact of interface design for building trust in mobile and factors distressing the mobile commerce implementation. In design, esthetics elements take account of color, photographs, layout and font style. In gaining trust, aspects like visual esthetics or website's design esthetics should be applied in making relationship with the consumer. viewed that design esthetics impinge on superficial effectiveness and effortlessness of website application.

Evidently, M-commerce differs from traditional e-commerce in terms of its user interface and its associated risk, interactivity, ubiquity, localization services, and usage patterns. M-commerce suffers from inherent limitations of small screen size, display of information, and security of transactions; nevertheless, it also provides opportunities for making transactions on the go. It comes with usability issues and restrictions, therefore, the factors influencing trust and the consequences of trust might differ across these platforms.

The ubiquity of mobile devices encourages consumers spontaneous purchase behavior which leads to enhanced sales for the seller. However, the nature of mobile technology inherently increases the risks and uncertainty of making purchases online as it distances the user from the service provider. Consumers experience high privacy and security risks due to the transmission of transaction data in a wireless environment. Trust plays an important role in diminishing the adverse effects of risk perceptions in m-commerce.

In conclusion, researchers believe that trust is associated with perceived privacy and security [4].

2 Domain Specifications

This topic involves specifying the construct domain of perceived security by developing the theoretical definition and identifying the different conceptual dimensions. The degree to which the online buyer believes that conducting an online transaction on the seller's website is safe in a manner consistent with the buyer's confident expectations. What are the primary relevant dimensions of perceived security?
After examining issues in security, which includes not only perceived security but also objective security. The findings reveal that confidentiality, integrity, and availability are the earliest and most widely used dimensions. Recent studies have added non-repudiation, authentication, access control, communication security, and privacy to the original triad.
Evaluating these dimensions using relevance, non-redundancy, and completeness as criteria for inclusion. Relevance refers to the dimension being consistent with the definition and characterizes the essence of perceived security. Non-redundancy refers to the fact that the dimension should not overlap with another dimension. Completeness ensures that all relevant and non-redundant dimensions have been included.
Based on these criteria, we select confidentiality, integrity, availability, and nonrepudiation as focal dimensions of perceived security [5].

Confidentiality. Confidentiality refers to the degree to which improper disclosures of information are anticipated and prevented. Systems with superior confidentiality are better able to anticipate and prevent improper disclosure of information, such as leakage of information to an unauthorized party. A system's inability to anticipate and prevent improper disclosure of information may well indicate system insecurity. Common security measures to maintain confidentiality include encryption and authentication such as password-based and token-based authentication.

Integrity. Integrity refers to the degree to which improper modifications to information are anticipated and prevented. Systems with superior integrity are better able to anticipate and prevent improper modification of information, such as faulty alteration, deletion, or addition. While some erroneous modifications of information are accidental, others may be made intentionally by unauthorized parties. Common security measures to maintain integrity include digital signatures and anti-virus programs that prevent a virus from destroying data.

Availability. Availability refers to the degree to which information is available to authorized subjects when required. Systems with superior availability are better able to consistently provide relevant information to authorized parties. Common security measures to maintain availability include back-up systems and countermeasures for distributed-denial-of-service attacks.

Non-repudiation. Non-repudiation in a buyer-seller exchange refers to the degree to which the systems can ensure that information sent by the customer is received by the person the seller claims to be. The goal is to ensure that the seller cannot later deny a completed transaction. Systems with superior non-repudiation are better able to provide verifiable proof of identity. Digital signature is a common security measure used to ensure non-repudiation.

Dimensions dropped due to their inconsistency with definition of perceived security are authentication, access control, and communication security. These variables more appropriately represent countermeasures to protect information assets from security attacks. Privacy is also excluded because researchers tend to conceptualize privacy as being distinct from security.

Based on the framework of four dimensions, we develop a measure of perceived security as a second-order construct with four first-order formative dimensions: perceived confidentiality, perceived integrity, perceived availability, and perceived non-repudiation. The specific definition for each dimension is presented in Table 1.

Table 1. Definitions of Constructs

Constructs	Definitions
Confidentiality	Online buyer’s belief that his/her transactional information will not be disclosed to unauthorized party
Integrity	Online buyer’s belief that his/her transactional information will not be altered by unauthorized party
Availability	Online buyer’s belief about the online seller’s ability and willingness to make information available to authorized subjects when required
Non-Repudiation	Online buyer’s belief that the online seller cannot afterward deny the transaction that has been performed

3 Trust factors in Mobile Commerce

In this topic it will be mentioned factors more focused on M-commerce and discussed how they affect user's feeling of security while using a mobile application, so that they will be more likely to use it again.

3.1. Technology acceptance factors

3.1.1. System quality. System quality is defined as the perceived quality exhibited in a system's overall performance. Due to the facelessness of mobile platforms, the access speed, navigation and visual appeal influence the users' first impression. Multiple m-commerce studies found that users tend to develop the high level of trust on a system when they perceive the system to be of high quality, which encourages them to spend more on that particular system.

3.1.2. Information quality. Information quality reflects the relevance, sufficiency, accuracy, and timeliness of the information provided by m-commerce systems. Users search for various information while using any m-commerce services. Inaccurate or out-of-date information undermines users' experience and signals that the system is incapable of providing timely and quality services, which further affects their trust in the system [6]. Extant research has highlighted the importance of information quality on trust in ecommerce, mobile banking, and financial services. Across different studies in m-commerce, researchers have found that trust is significantly influenced by the information quality. Thus, the following hypothesis is proposed:

There is a significant, positive relationship between information quality and trust in m-commerce.

3.1.3. Service quality. Service quality reflects the ability of a system to provide reliable, responsive, assured and personalized offerings to the users. Reliable and efficient service provides a sense of high quality which enables the users to build trust in the system [7]. Existent literature has found service quality as a determinant of users' trust. When service quality experienced by the users exceeds a certain level, users form trust as they perceive the service provider to be competent. However, untimely and unreliable services build distrust in the users about the system. Hence, we get that:

There is a significant, positive relationship between service quality and trust in m-commerce.

3.1.4. User interface. User interface in m-commerce refers to the user environment (such as menus, options, and various functions) for controlling the mobile devices. Previous studies on trust formation in m-commerce revealed that user interface is an important determinant of users' trust in the system. Well-designed user interface reduces the perceived system complexity, facilitates navigation and interactivity, and makes the users trust the system [8].

3.2. Risk factors

3.2.1. *Perceived risk.* Perceived risk is defined as the users' subjective evaluation of incurring losses while using a system. In 2017 researchers used perceived uncertainty as their study variable to examine the perceived risk associated with loss of privacy and security [9]. In a mobile environment, users are affected by a sense of insecurity due to potential undesirable behavior related to unauthorized access to their personal or financial data. Lack of information concerning data security makes the users hesitant of using mobile technologies as it is perceived to be risky. Research suggests that trust is affected by perceived risk.

3.2.2. *Individual factor: disposition to trust.* Disposition to trust remains stable over time in an individual and refers to the ability of an individual to form trust in general. Due to differences in disposition to trust, individuals tend to develop trust differently under the same circumstances. Individuals across different cultures with different life experiences differ in their disposition to trust. It is shaped as a result of personality types, experiences, and background. Several researchers in the domain of m-commerce found that an individual's disposition to trust has a direct effect on the formation of trust [10].

3.2.3. *Structural assurance.* Structural assurance refers to the existence of technological and legal structures that safeguard. It represents an institution-based mechanism and provides assurances related to confidentiality and protection of information. In the context of m-commerce, structural assurance in the form of promises, guarantees, regulations, insurances, and contractual terms and conditions signals credibility of the vendor and helps in building trust in the system [11]. Many prior researchers found that structural assurance leads to trust among users.

3.2.4. *Ubiquity.* Ubiquity refers to the ability of users to conduct business activities or transactions using their mobile devices at anytime from anywhere. Mobile technology enables users to minimize the temporal and spatial constraints by providing an opportunity to conduct ubiquitous transactions. However, ubiquitous connectivity may be hindered as a result of poor connectivity and service failures [12]. Such service interruptions lead to users' frustration and dissatisfaction which ultimately impact the user experience. Contrary to that, ubiquitous connectivity signals vendors' ability to providing efficient service which further fosters users' trust in the platform.

In conclusion, all factors discussed previously influence an individual's capability of trusting a mobile platform, specially security concepts that are meant to protect not only users but information and critical data from the sellers. Good consequences can reflect from feeling safe while using an electronic commerce platform like user satisfaction and loyalty towards a trusted platform which will translate in the likelihood of a user coming back to buy from the seller.

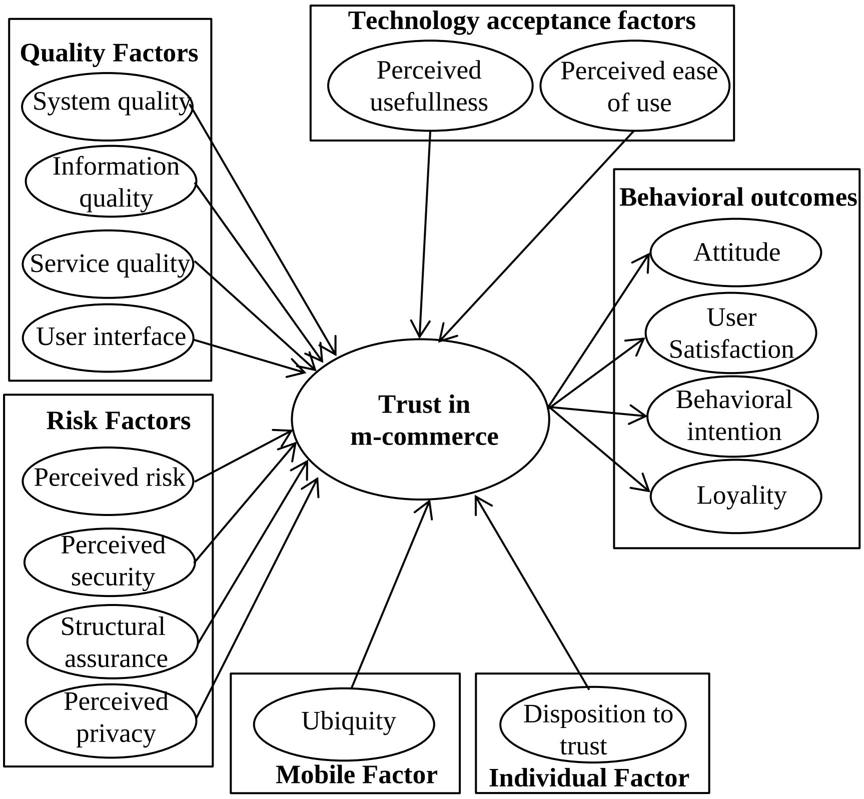


Fig 1. Relationships that influence trust

4 Defending Information Systems and E-Commerce

Defending information systems regardless of their nature is similar, the objective is keeping information secure, physically and digitally.
There are a lot of techniques to do so and this topic will only highlight a few of the security measures, dividing it into three categories: Access control, encryption, and PKI, Security in e-commerce networks, and General protection and social engineering.

4.1 Access Control, Encryption, and PKI

Access control determines who (person, program, or machine) can legitimately use the organization’s computing resources (which resources, when, and how). Access control involves ***authorization*** (having the right to access) and ***authentication***, which is also called user identification (user ID), i.e., proving that the user is who he or she claims to be. Each user has a distinctive identification that differentiates it from other users. Typically, user identification is used together with a password.

After a user has been identified, the user must be ***authenticated***. Authentication is the process of verifying the user's identity and access rights. Verification of the user's identity usually is based on one or more characteristics that distinguish one individual from another.

Biometric Systems

A biometric authentication is a technology that measures and analyzes the identity of people based on measurable biological or behavioral characteristics or physiological signals. Biometric systems can identify a previously registered person by searching through a database for a possible match based on the person's observed physical, biological, or behavioral traits, or the system can verify a person's identity by matching an individual's measured biometric traits against a previously stored version. Examples of biometric features include fingerprints, facial recognition, DNA, palm print, hand geometry, iris recognition, and even odor/scent. Behavioral traits include voice ID, and signature verification [13].

Encryption and the One-Key (Symmetric) System

Encryption is the process of encoding data into a form (called a ciphertext) that will be difficult, expensive, or time-consuming for an unauthorized person to understand. All encryption methods have five basic components: plaintext, ciphertext, an encryption algorithm, the key, and key space. Plaintext is a human-readable text or message. Ciphertext is an encrypted plaintext. The encryption algorithm is the set of procedures or mathematical algorithms used to encrypt or decrypt a message. Typically, the algorithm is not the secret piece of the encryption process. The key (key value) is the secret piece used with the algorithm to encrypt (or decrypt) the message.

Encryption has two basic options: the symmetric system, with one secret key, and the asymmetric system, with two keys.

Public Key Infrastructure

A public key infrastructure (PKI) is a comprehensive framework for securing data flow and information exchange that overcomes some of the shortcomings of the one-key system. For example, the symmetric one-key encryption requires the writer of a message to reveal the key to the message's recipient. A person that is sending a message (e.g., vendor) may need to distribute the key to thousands of recipients (e.g., buyers), and then the key probably would not remain secret. The PKI solution is using two keys, public and private, as well as additional features that create a highly secured system. In addition to the keys, PKI includes digital signatures, hash digests (function), and digital certificates [14].

Digital Signatures and Certificate Authorities

Digital signatures are the electronic equivalent of personal signatures on paper. They are difficult to forge since they authenticate the identity of the sender that uses the public key. Digital signatures are legally treated as signatures on paper.

Secure Socket Layer

PKI systems are further secured with SSL: A protocol for e-commerce. The PKI with SSL makes e-commerce very secure but cumbersome for users. One of the major protocols in use today is Secure Socket Layer), which has been succeeded by Transport Layer Security (TLS based on SSL).

4.2 Securing E-Commerce Networks

Several technologies exist that ensure that an organization's network boundaries are secure from cyberattack or intrusion, and that if the organization's boundaries are compromised, the intrusion is detected quickly and combated.

Firewalls

Firewalls are barriers between an internal trusted network (or a PC) and the untrustworthy Internet. A firewall is designed to prevent unauthorized access to and from private networks, such as intranets. Technically, a firewall is composed of hardware and a software package that separates a private computer network (e.g., your LAN) from a public network (the Internet). Firewalls are designed mainly to protect against any remote login, access by intruders via backdoors, spam, and different types of malware (e.g., viruses or macros). A popular defense system is a DMZ. The DMZ can be designed in two different ways, using a single firewall or with dual firewalls [15].

The Dual Firewall Architecture: The DMZ

In the DMZ architecture (DMZ stands for demilitarized zone), there are two firewalls between the Internet and the internal users. One firewall is between the Internet and the DMZ (border firewall) and another one is between the DMZ and the internal network. All public servers are placed in the DMZ (i.e., between the two firewalls). With this setup, it is possible to have firewall rules that allow trusted partners access to the public servers, but the interior firewall can restrict all incoming connections.

Virtual Private Networks (VPNs)

A virtual private network refers to the use of the Internet to transfer information, but in a more secure manner. A VPN behaves like a private network by using encryption and other security features to keep the information secure. For example, a VPN verifies the identity of anyone using the network.

Intrusion Detection Systems (IDS)

No matter how protected an organization is, it still can be a target for attempted security attacks. For example, most organizations have antivirus software, yet they are subjected to virus attacks by new viruses. Therefore, an organization must continually monitor for attempted, as well as actual, security breaches. The monitoring can be done by using intrusion detectors. An intrusion detection system (IDS) is a device composed of software and/or hardware designed to monitor the activities of computer networks and computer systems in order to detect and define unauthorized and malicious attempts to access, manipulate, and/or disable these networks and systems.

Dealing with DoS Attacks

DoS attacks are designed to bombard websites with all types of useless information, which clogs the sites, detecting an intrusion early can help. Since there are several types of DoS attacks (e.g., DDoS), there are several defense methods. Intrusion detecting software (mentioned previously) also identifies the DoS type, which makes the defense easier and faster [16].

4.3 General Protection, Spam, and Social Engineering Controls

The objective of IT security management practices is to defend information systems. A defense strategy requires several controls.

The major types of controls are: (1) General controls, which are designed to protect all system applications. (2) Application controls guard applications. In this and the following sections, we discuss representative types of these two groups of information system controls. Later in the section, we cover spam and fraud mitigation.

Protecting Against Spam

Sending spam that includes a sales pitch and looks like personal, legitimate e-mail and may bypass filters is a violation of the U.S. Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003. However, many spammers hide their identity by using hijacked PCs or spam zombies to avoid detection and identification. For protecting your system against botnet attacks, which also spread a huge volume [17].

Business Continuity and Disaster Recovery

Disasters may occur without warning. A prudent defense is to have a business continuity plan, mainly consisting of a disaster recovery plan. Such a plan describes the details of the recovery process from major disasters such as loss of all (or most) of the computing facilities or the data.

Example: Hospital Paid Ransom after Malware Attack Hollywood Presbyterian Medical Center paid a ransom of $17,000 in Britain (so the) blackmailer-hacker cannot be identified. The hacker encrypted the data that were not backed up. The hospital failed with its disaster recovery plan, so there was no choice (per the hospital management) but paying the ransom [18].

4.4 Why Is It Difficult to Stop Internet Crime?

The following are the major reasons Internet crime is so difficult to stop.

Making Shopping Inconvenient: Strong EC security may make online shopping inconvenient and may slow shopping time as well. Therefore, shoppers may not like some security measures
Shoppers' Negligence: Many online shoppers are not taking the necessary (but inconvenient) precautions to avoid becoming victims of identity theft or fraud.
Design and Architecture Issues: It is well known that preventing vulnerability during the EC design and pre-implementation stage is far less expensive than mitigating problems later; unfortunately, such prevention is not always made.
Ignoring EC Security Best Practices: Many companies do not have prudent IT security management or employee security awareness. Many widespread threats in the United States stem from the lack of user awareness of malware and hacking attacks [19].

5 Conclusion

In this paper the issue of e-commerce and m-commerce security was investigated, not only from the developer perspective, but also keeping in mind the user experience and their requirement for a platform to be trusted.
In addition, there were clarified many terms that are often used when talking about security in computer science, and more specifically what they differ when compared in m-commerce vs e-commerce.
Comprehending the topics on this study it is fair to state that as long as the internet remains insecure, it is virtually impossible to authenticate the other party to a transaction.
In conclusion, digital security is an ongoing evolving subject, and every day there are new methods to exploit breach platforms but there are also new ways to defend them, and all signs lead to it remaining this way.

References

1. E-commerce statistics for individuals, Eurostat from Information and communication technology, 2019
2. Popularity contest between E-Commerce and Traditional Retail Business, from International Journal of Technology for Business, 2019
3. Mehrbakhsh Nilashi, Othman Ibrahim, Vahid Reza Mirabi, Leili Ebrahimi, Mojtaba Zare.: “The role of Security, Design and Content factors on customer trust in mobile commerce” in Journal of Retailing and Consumer Services, 2015
4. Subhro Sarkara, Sumedha Chauhan, Arpita Khare.: “A meta-analysis of antecedents and consequences of trust in mobile commerce” in International Journal of Information Management, 2019
5. Edward Hartono, Clyde W. Holsapple, Ki-Yoon Kim, Kwan-Sik Na, James T. Simpson.: “Measuring Perceived Security in B2C Electronic Commerce Website Usage: A Respecification and Validation” in Decision Support System, 2014
6. Silic, M., & Ruf, C. The effects of the elaboration likelihood model on initial trust formation in financial advisory services. International Journal of Bank Marketing, 2018
7. Wang, W., Ou, W., & Chen, W. The impact of inertia and user satisfaction on the continuance intentions to use mobile communication applications: A mobile service quality perspective. International Journal of Information Management, 2018
8. Stewart, H., & Jürjens, J.: Data security and consumer trust in FinTech innovation in Germany. Information and Computer Security, 2018
9. Rana, N. P., Barnard, D. J., Baabdullah, A. M. A., Rees, D., & Roderick, S.: Exploring barriers of m-commerce adoption in SMEs in the UK: Developing a framework using ISM. International Journal of Information Management, 2019
10. Matemba, E. D., & Li, G. Technology in Society Consumers’ willingness to adopt and use WeChat wallet: An empirical study in South Africa. Technology in Society, 2018
11. Oliveira, T., Faria, M., & Abraham, M.: Extending the understanding of mobile banking adoption: When UTAUT meets TTF and ITM. International Journal of Information Management, 2014
12. Lin, H.-F.: An empirical investigation of mobile banking adoption: The effect of innovation attributes and knowledge-based trust. International Journal of Information, 2011
13. Wang, S. W., Ngamsiriudom, W., & Hsieh, C.: Trust disposition, trust antecedents, trust, and behavioral intention. Service Industries Journal, 2015
14. Scott, J. Cybersecurity 101: What You Absolutely Must Know! - Volume 1: Learn to be Pwned, Thwart Spear Phishing and Zero Day Exploits, Cloud Security Basics, 2016
15. Teo, F. “Monitoring Your Internal Network with Intelligent Firewalls.” Enterprise Innovation, 2016.
16. Teo, F. “Monitoring Your Internal Network with Intelligent Firewalls.” Enterprise Innovation, 2016
17. Alison Quine in: “How to Prevent Denial of Service Attacks”, 2008
18. Lenovo. “Lenovo Recommends 15 Steps to Reducing Security Risks in Enterprise Mobility.” White Paper, 2013.
19. Smith, C. “It Turns Out Target Could Have Easily Prevented Its Massive Security Breach.” March 13, 2014. bgr.com/2014/03/13/targetdata-hack-how-it-happened, 2016

Major Challenges in Digital Contents Copyright Protection

André Fontes

Lusófona University of Porto,
R. Augusto Rosa 24, 4000-098 Porto, Portugal

arkelogen98@gmail.com

Abstract. The advances of technology can put the Digital Content creators in a bad position because how easy it is for "pirates" to make illegal perfect copies of videos, images, artistic work, literature, documents and among other subjects. This is a violation of copy right ownership therefor there are some people that focus on protecting the copyrights like Digital Rights Management (DRM). The DRM focus on restricting the digital copy while securing and administering copyrights and their trademarks to the extent permitted by copyright laws. It is currently possible to customize the retail spread of a commercialized file, for example by limiting the number of times that file can be opened or the duration of its validity. This Paper reports how DRM is used by content holders, how DRM try to ease the practice of piracy, other types of protection that content holders can do, discuss the fair use and not fair use of digital content. This paper will also report about watermark and security of content.

Keywords: Copyright, Digital Content, DRM, Fair use, Licenses, Progressive download, Piracy

1 Introduction

The increase of digital content and the advance of multimedia bring opportunities for content creators to publish their work and to be recognized.[1] The problem behind the digital content now is how easy it is to make perfect illegal copies and to distribute to others through internet. The internet now is used for everything, publish works from school, articles, artist work, among others which make more vulnerable the content that is private, that someone has ownership like producers. That's why it should be license control of downloads and copying copyright content because now it's more difficult to producers to sell their information and content at a profitable price. The digital information its not only distributed in the internet but may be also distributed by email, even people can use spoofing to capture information that is not theirs and use it to is on benefit.

10.11228/dpsc.02.01.008

Nowadays authors request copyright protection of digital content so that web users can be restricted and not distribute the digital content as he like and to protect the originality and creativity of their intellectual properties.[1]

One way to protect the copyright is to use the Digital Rights Management (DRM) which use the laws to enforce the copyrights and restricting the use of digital content. The DRM can have problems related to “fair use” and privacy because the DRM need a specific legal measures and contractual mechanisms in order to regulate the “fair use” and minimize privacy conflits.

The second topic will report about copyright, piracy, fair use and how these 3 topics are related.

The third topic will report about Digital Rights Management, how it works, what are the advantages and disadvantages.

The fourth topic will report about solutions to the copyright protection and to complement the DRM systems.

2 Copyrights

Copyright is the exclusive right that a creator or a producer have over of a type of work or content like a music, video games, movies among others.

The term of copyright for a work depends on several factors, including whether it has been published, and, if so, the date of first publication. As a rule, for works created after January 1, 1978, copyright protection lasts for the life of the author plus an additional 70 years.[2]

The term Copyright came with the objective to reward a content creator for his work and his originality but with the internet in the mix also came the pirates, who use content from the copyright owners to his own benefit because now is easy to create copies of a type of content and distribute them like copies of a music.

Copyright protection rules are similar worldwide, due to several international copyright treaties, the most important of which is the Berne Convention. Under this treaty, all member countries — and there are more than 100, including virtually all industrialized nations — must afford copyright protection to authors who are nationals of any member country. This protection must last for at least the life of the author plus 50 years and must be automatic without the need for the author to take any legal steps to preserve the copyright.[3]

2.1 Piracy and Fair Use

Piracy is an illegal act that people do to obtain content that is not theirs and by doing that they violate de laws of copyright.

There are two basic ways in which piracy can occur [4]:

- Unauthorized acquisition. This form of piracy occurs when a consumer obtains copyrighted content illegitimately, for example, by an unauthorized download of content from a peer-to-peer file sharing service, such as Gnutella, or by obtaining illegitimate CDs or DVDs from a street vendor of friend.

- Unauthorized use. This form of piracy occurs when a consumer obtains a piece of copyrighted content legitimately and then attempts to use it in an unauthorized way.

Namely all forms of digital piracy are, to some extent, associated because they are inversely correlated to wider measures of socioeconomic development, the richer the country, the lower its piracy rate.[5]

Economic models of piracy in general study the impact of piracy on profits and the effect of enforcing copyright. Conventional wisdom suggest that piracy represents a drain to publisher profits and reducing piracy forces consumer to legitimately acquire software. We then identify various scenarios including the existence of domestic software industry and study their effect on government incentive for increased copyright enforcement and publisher profits.[6]

The importance of ethics in modelling software piracy is a recurring theme that is just beginning to be tapped. The decision to copy or not copy intellectual property is influenced by ethical reasons. Ethics is the study of moral systems. It is important to note that the moral philosophers do not make moral judgments about right or wrong but attempts to discover truth about the meanings of concepts and justification of judgments.[6]

In the digital environment, the consumer's right to be anonymous in purchasing music, products or services has been severely hampered. The Digital Rights Management software requires users to register their email addresses and other personal information as part of authorization and verification.[7]

The history of "fair use" extends far back before PD 49 and the 1997 Copyright Law.US and Philippine courts, in the past, allowed certain, limited uses of copyrighted material without permission from the copyright owner. Consequently, in the process, these courts, by precedent, firmed up the practice of fair use privilege. The doctrine provides freedom to make copies and publish quotations beyond the special privileges granted to libraries and archives. In time, "fair use" became a convenient excuse for copying, and served as a defence against copyright infringement, when invoked. The doctrine also permits libraries to supply multiple copies of materials for classroom teaching, for purposes of scholarship, research and private study, criticism and review, news reporting, and similar purposes.[8]

3 Digital Rights Management

The goal of a distributed DRM system is for content authors to be able to project policies governing their content into remote environments with confidence that those policies will be respected by the remote nodes.[9]

First, DRM is about managing the policies under which material will be made available, and then it is about ensuring that these policies are respected.[9]

Unfortunately, today, with a simple browser plug-in, in many sites you can download available material, so it's not uncommon to find courses, movies, and music being marketed illegally or in districts.

DRM can be used to detect and verify ownership of data and to control access to the data in accordance with a policy determined by the content creator or distributor. A further approach frequently incorporated in a DRM system to embed a digital watermark in the digital media file.[10]

DRM removes usage control from the person in possession of digital content and puts it in the hands of a computer program. The applications and methods are endless, here are just a few examples of digital rights management [11]:

- A company sets its servers to block the forwarding of sensitive e-mail.
- An e-book server restricts access to, copying of and printing of material based on constraints set by the copyright holder of the content.
- A movie studio includes software on its DVDs that limits the number of copies a user can make to two.
- A music label releases titles on a type of CD that includes bits of information intended to confuse ripping software.

DRM systems must also facilitate the delivery of content offline on CDs and DVDs, deliver content on-demand over peer-to-peer networks, enterprise networks, or the Internet and provide ways of determining the authenticity of content and of rendering devices.[12]

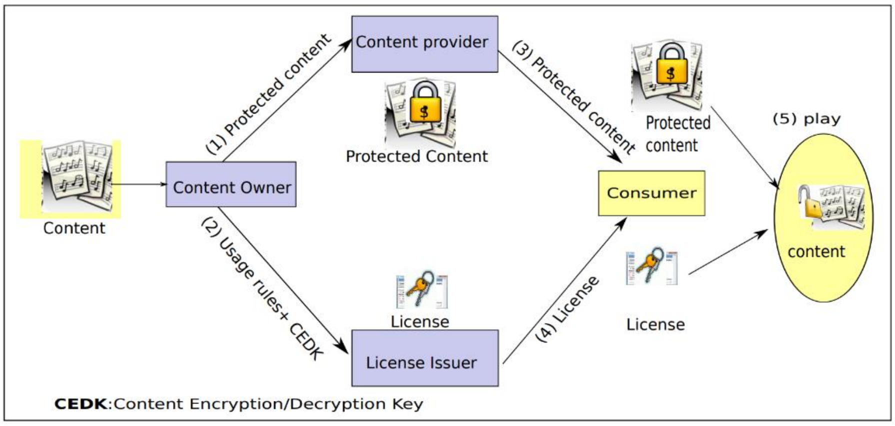


Fig 1. Typical DRM system architecture [13]

The digital content is packaged (encrypted and metadata enriched) and then provided through distribution channels. Users need special controllers (client-side s/w) in order to be authenticated and gain access through the decryption of content. License servers may be used to manage licenses describing access rights and conditions.[14]

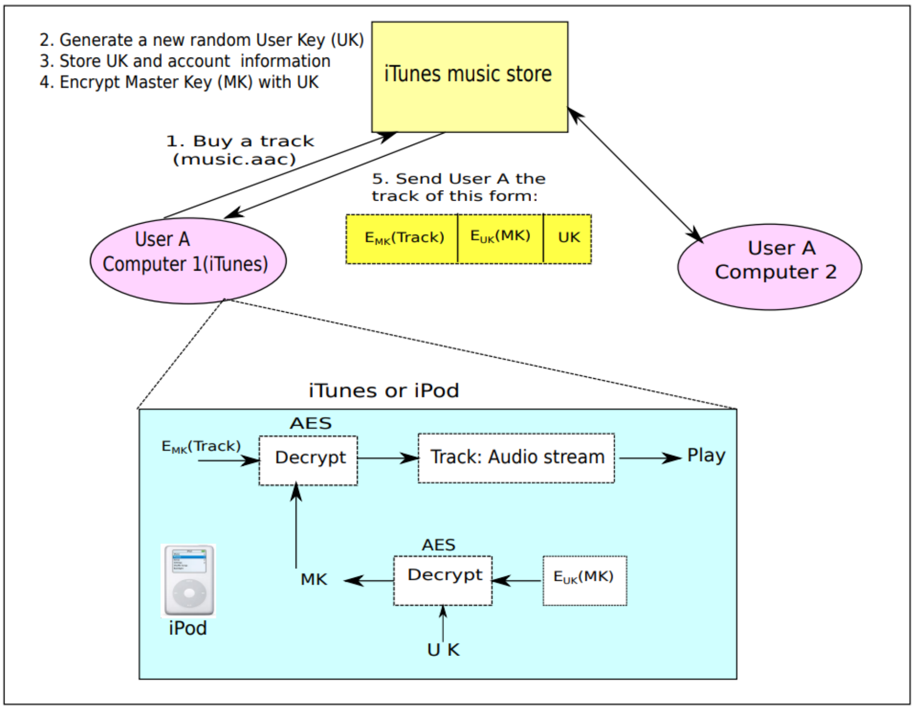

2. Generate a new random User Key (UK)
3. Store UK and account information
4. Encrypt Master Key (MK) with UK
iTunes music store
1. Buy a track (music.aac)
5. Send User A the track of this form:
E_MK(Track)
E_UK(MK)
UK
User A Computer 1(iTunes)
User A Computer 2
iTunes or iPod
AES
E_MK(Track)
Decrypt
Track: Audio stream
Play
AES
MK
Decrypt
E_UK(MK)
U K
iPod

Fig 2. Dataflow of Apply Fair Play DRM [13]

Apple enforced DRM despite not being the actual creator or owner of the intellectual property it licensed. This placed it in the awkward position of maintaining the DRM despite having only marginal, or tangential stake in that IP beyond its role as a gate-keeper. This ultimately contributed to its decision to back down from its DRM scheme.[15]

The big problem of DRM its that it takes control of the content and places a lot of processing issues but brings security to the content providers and tries to end the piracy although its impossible to end that.

4 Solutions that improve copyright protection

4.1 Watermark and fingerprint

Other type of solutions for digital content protection is the scheme of watermark. A watermark is a signal added to some form of digital data (music, video, image) that can make you prove that you are the owner of that product, its very hard to remove the watermark by distorting the image and its difficult to find the watermark if you don't know the secret key.

The Watermark tactic it's an attribution of a private key to an original digital data that if other people try to claim that digital data, the owner can produce the unmarked original and demonstrate the presence of her watermark in the image that the other people are trying to claim.

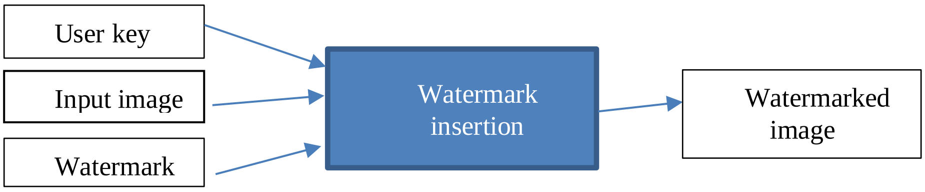


Fig 3. Representation of watermark insertion

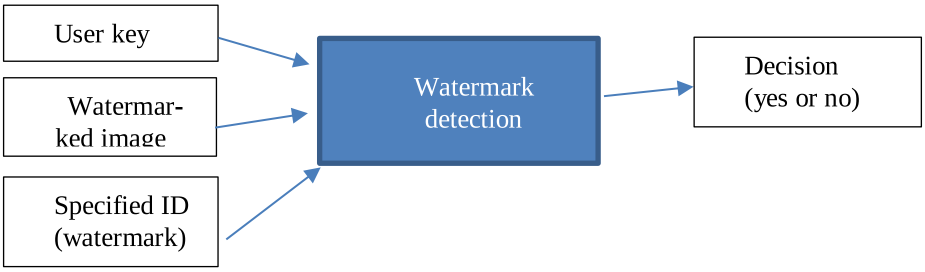


Fig 4. Representation of watermark detection

The digital watermarking system essentially consists of a watermark encoder and a watermark decoder. The watermark encoder inserts a watermark onto the host signal and the watermark decoder detect the presence of watermark signal.

The encoder process is the attribution of a private key to the image and generate de image with the watermark posted. The decoder process is the opposite it takes the image with or without the watermark and compares with the other image.

For this technique you can make an algorithm that helps you restrain and detect if people are stealing your content.

The watermark can also be used to content protection, when a content creator wants to sell his product, this technique can be used to protect the work. It can also be used, with some software, to limit the number of copies permitted. Every time a copy is made, the watermark can be modified by the hardware and at some point the hardware would not create any more copies of the data. An example is the digital video disc (DVD).

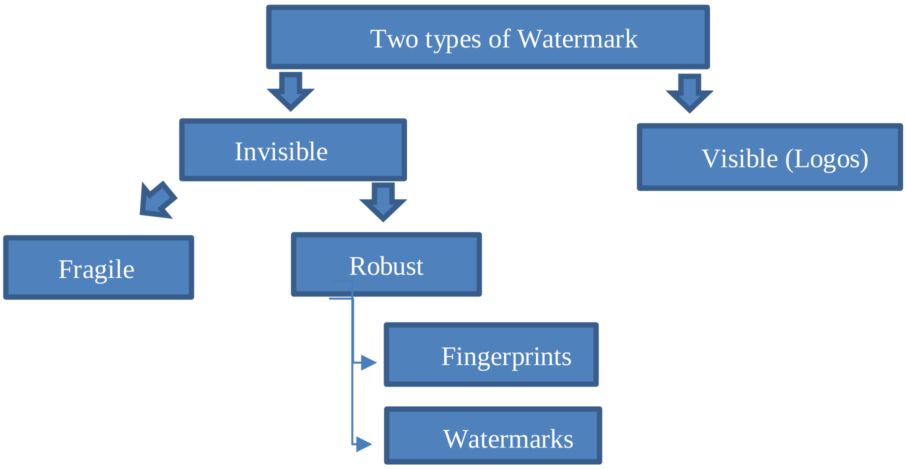


Fig 5. Representation the two types of Watermark

There are two types of watermark, the visible watermark corresponds to logos that you usually see during the video or an image, the invisible watermark corresponds to the watermark that are in embedded on the image that only with software can you see the watermark. In the invisible watermarks there are the fragile watermark which is used for detecting the smallest alteration of an image, while the robust watermark is specially designed to withstand a wide range of "attacks", which basically are trying to remove the watermark, but without destroying the image/video.

Fingerprinting is different of the basic watermark that embed information on the digital data, the fingerprinting analyses the image or video and determine the unique characteristics. These characteristics when are identified they are put on a database and then are use for recognizing the content in the future. Normally it only is few samples of the video that are store in the database because if it was a full video it would make a lot of samples that you would have to store, and it would make it heavier and take a lot of time to verify the fingerprint. The fingerprinting can be often use in forensics for detecting if the video footage was manipulated.

YouTube permit that content owners to fingerprint their own media and then upload to the database of YouTube. That way YouTube can compare with central fingerprinting database before the video can be viewed. If someone uploads a piece of content that its original owner requested be blocked, then YouTube will not allow this video to be shown. Copyright owners get to decide what happens when content in a video on

YouTube matches a work they own. They can block it, monetize the video by running ads against it or track the video's viewership statistics.

An easy way to watermark an image is to change the position of the pixels, that alone creates a new image. Digital Watermarking doesn't stop piracy but at least brings some protection for content holders and providers because it needs some knowledge to take the watermark out from an image or a video.

I decided to talk about watermarking because nowadays is very common to use this technique, for example on the platform YouTube there is a section that can create your watermark and you also can modify the watermark at your own taste.

There is also, to protect your own work, companies that takedown websites that use content that is not theirs, but those companies need proves that you are the content creator and for that you can use watermark as your evidence.

4.2 Protection of files

Nowadays streaming also has a big problem because there is no way to completely prevent online video from being stolen. If it can be viewed on a computer, it can be stolen. The best you can do is make it harder for thieves and minimize the number of times the video is stolen.

The transfer of media file from server to a client is termed as Progressive Download. There is low protection via Progressive Download, if it is used an embedded media player such as QuickTime or Windows Media player, the user can access the file directly by looking at the HTML code, by HTML code can be used to determine the location of the video file. To add a little security to progressive download, in the code the JavaScript should be on a JS file to be in a different location of the HTML file, so that becomes harder to thieves to find the files and you should use flash video because creates a SWF file that hides his location.

SWF file is an Adobe flash file format which contains videos and vector-based animations. The full abbreviation of SWF is Small Web Format but sometimes it is referred as Shockwave Format. SWF files are generally used for efficient delivery of multimedia contents over the web. This format can also contain ActionScript's, which come in handy in small web-based applications. This type of file is harder to open and see the information but only add a little security.

5 Conclusion

The objective of this paper is to present some tools to copyright protection and to bring some security to content holders.

With the advance of technology, it became easy for people to use other people content to their benefit, so that's why in this paper I present the DRM systems and watermarking. The DRM systems are more sophisticated but more secure that watermarking because DRM implements watermarking and more types of techniques to secure the content but for DRM to work it needs to take control of the content as it is refereed in the paper.

Watermarking and Fingerprinting it's easier to implement and it is effective because removes many people for trying to steal content. With these techniques you can provide a secure environment for people to be in like YouTube.

The paper presents solutions for copyright, but the society will always be the factor that controls everything because there are always people that can break the barriers so it will depend of the ethic of the society.

Piracy will always exist no matter what because systems always have flaws.

References

1. Dan Jerker B. Svantesson & Stanley Greenstein (editors), Data protection vs. copyright, Internationalisation of Lawin the Digital Information Society, Nordic Yearbook of Law and Informatics 2010-2012, https://ssrn.com/abstract=2350131
2. copyright.gov,https://www.copyright.gov/help/faq/faq-duration.html,consulted 20/10/2019
3. Stanford University Libraries, https://fairuse.stanford.edu/overview/faqs/copyright-protection/,consulted 22/10/2019
4. M. Campidoglio, F. Frattolillo, F. Landolfi, The Copyright Protection Problem: Challenges and Suggestions, Publisher: IEEE, https://doi.org/10.1109/ICIW.2009.84 (2009)
5. Antoni Terra, Copyright Law and Digital Piracy: An Econometric Global Cross-national Study. North Carolina Journal of Law & Technology. 18. 69. , 2006
6. Mrs. D. Seema Dev Aksatha, MCA, M. Blessing Marshal, Software Piracy Protection, https://doi.org/10.31142/ijtsrd21705 (2019)
7. Thishya Weragoda, Pirates of the Internet: The Curse of the Digital Age" Balancing and Protecting the Rights of Music Owners and Music Users in the Digital Environment, https://www.academia.edu/38153599/_Pirates_of_the_Internet_The_Curse_of_the_Digital_Age_Balancing_and_Protecting_the_Rights_of_Music_Owners_and_Music_Users_in_the_Digital_Environment (2016)
8. Fe Angela M. Verzosa, Copyright Protection for Philippine Publications, In 12th Congress of Southeast Asian Librarian (CONSAL) on Information Resources Empowerment, Brunei Darussalam (Philippines),19-23 October 2003.[Conference paper], http://hdl.handle.net/10760/11219
9. Charles Duncan, Ed Barker, Peter Douglas, Martin Morrey, Charlotte Waelde, Digital Rights Management, https://www.academia.edu/567801/Digital_rights_management (2004)
10. Ahmed Gomaa, Global Music Asset Assurance Digital Currency : A DRM Solution for Streaming Content Using Blockchain, Conference: 6th International Conference of Advanced Computer Science & Information Technology, https://airccj.org/CSCP/vol8/csit88801.pdf (2018)
11. JULIA LAYTON, https://computer.howstuffworks.com/drm1.htm consulted 19/11/2019
12. S.R. Subramanya and B.K. Yi, Digital rights management, Publisher: IEEE, https://doi.org/10.1109/MP.2006.1649008 (2006)
13. Tarek Gaber, Digital Rights Management: Open Issues to Support E-Commerce, DOI: 10.4018/978-1-4666-3954-6.ch005 (2013)

14. Athanassios Skodras,Vassilis Fotopoulos, Decentralising the Digital Rights Management value chain by means of distributed license catalogues, Publisher: Springer Boston MA, https://doi.org/10.1007/0-387-34224-9_81
15. Timothy J. Wade and S.R. Subramanya, Digital Rights Management in 3D Printing: A Proposed Reference Architecture for Design-to-Fabrication Security and Licensing, https://www.academia.edu/33225875/Digital_Rights_Management_in_3D_Printing_A_Proposed_Reference_Architecture_for_Design-to-Fabrication_Security_and_Licensing

Major Challenges in Digital Contents Copyright Protection

João Tomás Barros Barreira[1]

[1]Lusófona University of Porto, Portugal
tomas.barreira14@outlook.pt

Abstract. This work aims to study how major digital platforms deal with copyright protection in the year 2019 while also complying with many other regulations originating from different countries. Introducing firstly with a study case where it will be recognized what kind of regulations do digital platforms tend to comply with in order not to be held accountable with copyright claims and since digital content can be accessed worldwide, it will be presented a comparison between regulations from the United States of America and Europe. Finally, as per the addition of the new Copyright Directive in the Digital Single Market to Europe regulations, more accurately the Article 17, it will also be mentioned the conflict it came to with the American Safe Harbor Law.

Keywords: Copyright, Rights Protection, Digital Platforms, Digital Millennium Copyright Act, Fair Use, Safe Harbor, Information Society Directive, Exceptions and Limitations, Copyright in the Digital Single Market, Article 17.

1 Introduction

Digital content, also known as digital media, is anything that exists in the form of digital data. It is known, but not limited, to be digital files that can be uploaded, broadcasted or streamed to a cloud storage service, digital file-sharing platform or another computer.

With the evolution of technology, the meaning of the word copyright has also matured from being directly associated with the use of the printing press to today's definition.

"In an era of restriction, copyright was a permission. In an era of freedom, it became a restriction."[1]

Copyright is now defined by Lexico Dictionary as the exclusive and assignable legal right, given to the originator for a fixed number of years, to print, publish, perform, film, or record literary, artistic, or musical material [2].

Many people have the misconception that copyright is something you apply to, but the truth is, once you create something in a fixed form, in a range of media content, writing, visual art, etc. , you automatically have the copyright of that content.

10.11228/dpsc.02.01.009

Of course, that is not enough if you want to take legal action against someone who infringed on your copyright. For that, the copyright must be registered so it can be legally established with a date of creation, as well as have the creator as the copyright owner of the work.

Copyright Protection constitutes a wide range of content protection by various holders, and in this article will be given attention specifically to digital contents and to how digital platforms comply with the regulations that every country or country union imposes. Sector 2 will be detailing what regulations digital platforms follow, how they act to remove copyrighted content from their platforms and also tackling the matter of what should happen if copyright holders engage in abusive or improper conduct in exploiting or enforcing the copyright.

Sector 3 will start by explaining some United States Regulations such as the Digital Millennium Copyright Act, the Fair Use Doctrine and the Safe Harbor provision.

Proceeding with some European Regulations, such as the Copyright in the Information Society Directive, which also includes an “Exceptions and Limitations” clause.

It will be given a comparison between the previously stated countries' regulations. This Sector will be finalized with an interpretation of the newly added Article 17 to European Regulations.

2 Digital Platforms compliance with regulations

Every company has to follow their countries regulations, but what happens if one is multinational with millions of users around the world. This section will analyze what regulations these Digital Platforms follow, how they act when they have the need to remove Copyrighted works from their service, and it will be displayed a few examples of improper conduct on Copyright enforcement.

2.1 What regulations they follow

With the evolution of the Internet, people's understanding of its properties has also evolved. In a world where everything is connected the probability of a person using any type of copyrighted work has risen to a point where digital content provider platforms had to make drastic changes to their systems so they could detect that type of behavior, creating services and algorithms to follow the regulations they were set.

It's hard to express with accuracy which regulations they follow but, stating that Digital Platforms tend to obey the strictest or most advanced set of laws available from each country would be a fair assessment, as it would be easier to enforce the same rules universally.

If the previous statement is considered valid, the following two figures will present a possible before and after states, within a small sample of countries, where these countries have different Copyright Regulations and what happens after these laws are applied globally by Digital Platforms.

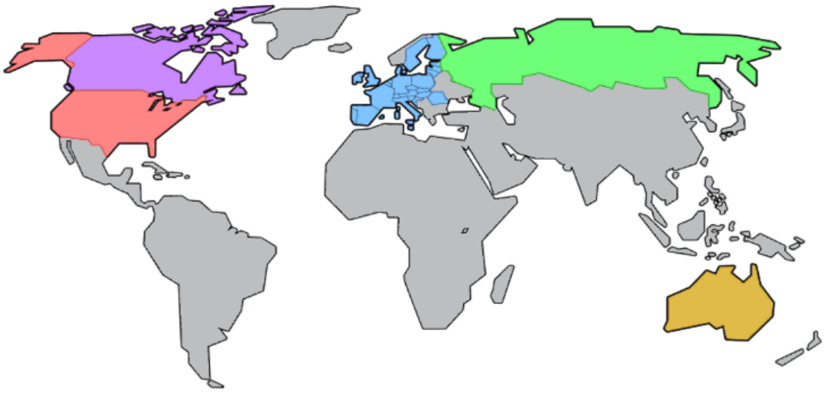


Fig. 1. Depiction of a few select Countries with different Copyright Regulations

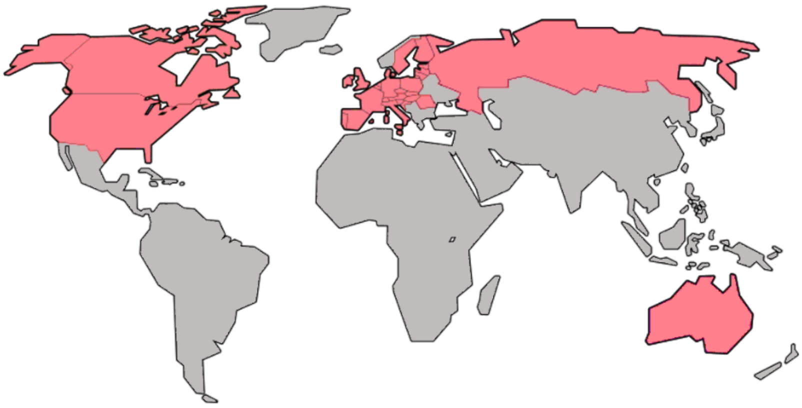


Fig. 2. Depiction of a few select Countries that were applied with the same Copyright Regulations globally by Digital Content Provider Platforms

Using the new General Data Protection Regulation (GDPR) as an example, Digital Platforms not based in the European Union would have no need to enforce this regulation if they had no clients who resided in the EU as written in Article 3 – Territorial Scope of the General Data Protection Regulation:

“2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."[4]

This regulation, once it was put into action, made a ripple effect on the internet. Every Digital Platform, even those not based in Europe, had to rewrite their privacy policies and, in turn, update the users of the changes to accommodate this new European directive.

2.2 How they act to remove copyrighted content

Using the platform YouTube as a study case, Copyright holders can use one of their services called Content ID "to easily identify and manage their content"[3] on the platform.

With this service, Copyright owners can choose one of three options, between:

- blocking a video from being viewed;
- monetizing the Video by running ads against it and in some cases sharing the revenue with the uploader; and
- tracking a video's viewership statistics. [3]

Copyright holders can also issue a takedown notice and, once it's complete and valid, YouTube has to remove the content as it's required by law. If the creator thinks the takedown was wrongfully issued, falling into the fair use doctrine, he can then send a counter-notification to the Digital Platform which forwards it to the person/company who requested the removal.

If there is an impasse between both parties, it would be up to them to settle the issue in court. [5]

2.3 Improper conduct on Copyright Enforcement

In the study case of YouTube, as this platform can't serve as a mediator, if the creator of content considers the content in question not in the right of being copyrighted, he can take the matter into court so it can be decided by an impartial jury.

For instance, until late 2018, Sony Music Entertainment was claiming 47 seconds of music from the composer Bach to anyone who posted it on Facebook. It is unclear whether it was caused by a takedown algorithm or an employee at Sony.[6] This displays a great example of how people or faulty algorithms can still make mistakes by copyrighting content from a Composer that died in the 1750s when it is known that Copyright Protections endures for the life of its owner with an additional 70 years.[7] It was also made known that the European Union was, at that time, debating the implementation of these algorithm filters "on all major technology platforms that host user content."[6] Concluding with a statement that if the proposal became law, "it was approved by the European Parliament on Wednesday"(at the time)[6], users could end up suffering from these mistakes more often.

3 United States and European relevant regulations

This section will analyze the most relevant regulations from the United States and Europe to the topic at hand and will also compare them.

3.1 United States Regulations

Digital Millennium Copyright Act (DMCA)

The Digital Millennium Copyright Act is a copyright law that "addresses the rights and obligations of owners of copyrighted material who believe their rights under U.S. copyright law have been infringed".[8]

But "With the continuing evolution of the digital age, the U.S. Copyright Office has gravitated from its original purpose of registering copyrights and serving as a copyright records office, to regulating copyright and copyright use through the implementation of laws, such as the DMCA"[9], not only including the discussed subject of this paper but also a wide range of Copyright and Security-related matters, such as the exception of Copyright for Security Testing which "permits circumvention of access control measures, and the development of technological means for such circumvention, for the purpose of testing the security of a computer, computer system or computer network, with the authorization of its owner or operator."[10].

On account of this copyright law, media companies are able to issue takedown notices to website owners, requesting the removal of infringing content on their website as written under Title II - Online Copyright Infringement Liability Limitation Act where "Under the notice and takedown procedure, a copyright owner submits a notification under penalty of perjury, including a list of specified elements, to the service provider's designated agent".[10]

While companies can issue takedown notices when their copyright is infringed, they also have to beware of existing exceptions, so that creators can make their content.

One of the main exceptions comes with the Fair Use Doctrine, which allows creators to use as a defense to copyright claims on the use of creative works.

Fair Use Doctrine

The United States Fair Use Doctrine would allow the use of copyrighted content for specific purposes with the intention of balancing copyright owners' interests with the public, to promote freedom of expression.[11]

This ruling, written in Section 107 of the Copyright Act "provides the statutory framework for determining whether something is a fair use "[11] while also identifying a few examples, such as criticism, comment, news reporting, teaching, scholarship, and research.[11]

When evaluating these activities to consider them as Fair Use, Section 107 considers four factors:

- Purpose and character of the use, including whether the use is of a commercial nature or is for nonprofit educational purposes; [11]
  - where courts verify how the party claiming fair use is using the copyrighted work. [11]
- Nature of the copyrighted work; [11]
  - This factor analyzes the degree to which the work that was used relates to copyright's purpose of encouraging creative expression. [11]
- Amount and substantiality of the portion used in relation to the copyrighted work as a whole; [11]
  - where courts look at both the quantity and quality of the copyrighted material that was used. [11]
- Effect of the use upon the potential market for or value of the copyrighted work;
  - In this last factor courts review whether, and to what extent, the unlicensed use harms the existing or future market for the copyright owner's original work.[11]

When the claimed content is deemed as "Fair" under Section 107 of the Copyright Act, the Digital Platforms are allowed to re-enable the display of the content in question.

Safe Harbor

Safe harbor is a provision of the "Online Copyright Infringement Liability Limitation Act"[10] that shields Digital Content providers from being liable for the infringing acts of Content Creators.

These Digital Content providers are considered only a middleman for their users, intending to provide a simpler and efficient way to share content not actively engaging in infringing activities whenever they happen, which means they should be protected against these actions.

According to the statute "Limitation for Information Residing on Systems or Networks at the Direction of Users"[10], Digital Content providers are eligible for this limitation when they meet one of the following conditions:

- "The provider must not have the requisite level of knowledge of the infringing activity, as described below;" [10]
- "If the provider has the right and ability to control the infringing activity, it must not receive a financial benefit directly attributable to the infringing activity;" [10]
- "Upon receiving proper notification of claimed infringement, the provider must expeditiously take down or block access to the material." [10]

3.2 European

Copyright in the Information Society Directive

The Information Society Directive is a regulation enacted by the European Union in 2001 to implement the World Intellectual Property Organization Copyright Treaty (WIPO Copyright Treaty).

This directive addresses and explains the definitions of the exclusive rights granted to copyright holders, differentiating article 2's "reproduction right" from article 3's "communication to the public".[11]

The fifth article covers "Exceptions and limitations" of this regulation expressing how these may apply to articles 2, 3 and 4. These constraints permit the use (in this case private copying) of copyrighted works under a certain amount of leniency, as said in addendum number 52 of the Information Society Directive: “Member States should likewise promote the use of voluntary measures to accommodate achieving the objectives of such exception or limitation”[13]. If these constraints are exploited, it could be provided legal action to cease any abusive activity.

The third point on the fifth article is the U.S. Fair Use Doctrine equivalent pointing out the exception cases where user created content are considered permitted, a few being:

- “the sole purpose of illustration for teaching or scientific research” [13] Article 5 3(a);
- “quotations for purposes such as criticism or review” [13] Article 5 3(d);
- “ use for the purpose of caricature, parody or pastiche” [13] Article 5 3(k);

Addendum 59 of the Information Society Directive includes that even in cases exempt under Article 5, Exceptions and Limitations, “rightholders should have the possibility of applying for an injunction against an intermediary who carries a third party's infringement of a protected work or other subject-matter in a network”[13].

3.3 Comparing United States and European regulations

United States and European regulations are similar in nature, both exercising the WIPO Copyright Treaty, which provides a “basis for the digital protection for the countries throughout the world through its convention and treaties”[14].

With the U.S. Digital Millennium Copyright Act, rightholders are able to perform Takedown Notices against the Copyright infringer which is processed by the Digital Platform, and, with the Information Society Directive, rightholders can file an injunction for the same purpose.

The Fair Use doctrine from Section 107 of the U.S. Copyright Act provides a list of exemplary exceptions where the use of copyrighted works is considered "fair".

The permitted "Exceptions" from Article 5 of the Information Society Directive present a list of "Exceptions and Limitations" where the use of copyrighted works is permitted.

Although similar, the European Copyright Directive becomes more restrictive because of the way it was written. Users could claim an alleged fair use right under DMCA regulations but that could not be deemed as such under EU's Copyright Laws.

3.4 Addition of Article 17 to European Regulations

As of June 2019, the Directive on Copyright in the Digital Single Market was published to complement and enforce a new set of jurisdictions on a few particular Directives: " 96/9/EC, 2000/31/EC, 2001/29/EC, 2006/115/EC, 2009/24/EC, 2012/28/EU and 2014/26/EU of the European Parliament and of the Council"[15].

This Directive was conceived with the intent to contribute "to the proper functioning of the internal market" and to stimulate innovation and creativity.[15]

This topic will focus on this regulation's article 17, which is the most relevant to the current work, and relevant paragraphs.

Article 17, "Use of protected content by online content-sharing service providers"[15], states that these Digital Platforms should "obtain an authorization from the rightholders" in order to share the content they hold with the public. In most platforms, this content is not always uploaded by them, which means they would have to be proactive to ensure that unauthorized copyrighted works would not be uploaded to their platform. This approach interferes with providers because no service or algorithm yet can have an accurate decision on this matter.

If no authorization is provided for such copyrighted works, Digital Platforms will be accountable for making the content public, unless they showed "efforts to obtain an authorization" or made their best by trying to remove the content from being online.[15]

This paragraph, 4, conflicts directly with the U.S. Safe Harbor provision making Digital Platforms liable of possible copyright infringing content that is being published in their service.

The sixth paragraph of the 17th Article is directed firstly to Digital Platforms that “have been available to the public in the Union for less than three years” [15] and have an annual turnover “below EUR 10 million”[15] and will have their conditions limited to paragraph 4.a, service providers demonstrate they have “made best efforts to obtain an authorization” [15] from the rightholders, after receiving a complete and valid notice “to disable access” to the content in question; secondly to such service providers where the "average number of monthly unique visitors" exceeds 5 million[15], they have to demonstrate that the best efforts were made to prevent further uploads of the content in question.

This action could hinder the service or algorithm used by the platform to monitor the contents they share over the internet because in the current state of technology it's very improbable that an algorithm can complete a scan of the content before it is shared on the platform.

The paragraph 7 emphasizes the “Exceptions and Limitations” still in action, with this Directive ensuring that “The cooperation between online content-sharing service providers and rightholders"[15] will not prevent these constraints from covering works that do not infringe copyright.

4 Conclusion

In this paper, was provided an explanation of how Digital Platforms should be applying their regulations on their services, how could they act to remove Copyrighted Content, and was shown an example of Improper Conduct on the Enforcement of Copyright. Afterward, it was made known about predominating Copyright Regulations from the United States and Europe, where they were explained and compared with each other, finishing with an explanation on the new Directive on Copyright in the Digital Single Market, specifically Article 17. This addition affected the security Digital Platforms had with the Safe Harbor Law, where they would not be condemned for their users' infringement.

Copyright Law was introduced firstly in 1710 in England, where it would acknowledge authors as the main beneficiary of this regulation. With only a duration of 28 years, at that time, copyright law rapidly grew to include new regulations and other types of creators, and by the 21st century, "more than 140 countries were party to the (Berne) convention"[16], formally known "as the International Convention for the Protection of Literary and Artistic Works."[16].

Nowadays, copyright law is an everyday occurrence, and it is applied to a wide range of content, not only on the internet and with various intentions. But the existence of different regulations to reach the same purpose have produced conflicts across countries that should be handled carefully when dealing with them.

References

1. Copyright Law In 2019, https://www.whoishostingthis.com/resources/copyright-guide/, last accessed at December 08th, 2019
2. Definition of Copyright by Lexico, https://www.lexico.com/en/definition/copyright, last accessed at November 26th, 2019
3. How Content ID works, https://support.google.com/youtube/answer/2797370?hl=en&ref_topic=9282364, last accessed at December 11th, 2019
4. European Parliament and Council of the European Union, Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Directive)
5. What is Copyright?, https://support.google.com/youtube/answer/2797466?hl=en, last accessed at December 12th, 2019
6. Sorry, Sony Music, you don't own the rights to Bach's music on Facebook, https://arstechnica.com/tech-policy/2018/09/sorry-sony-music-you-dont-own-the-rights-to-bachs-music-on-facebook/, last accessed at December 18th, 2019
7. How Long Does Copyright Protection Last?, https://www.copyright.gov/help/faq/faq-duration.html, last accessed at December 18th, 2019

8. What is DMCA?, https://www.dmca.com/faq/What-is-DMCA, last accessed at December 12th, 2019
9. Katherine Weigle, How the Digital Millennium Copyright Act affects Cybersecurity (2017)
10. 105th United States Congress, THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998
11. More Information on Fair Use, https://www.copyright.gov/fair-use/more-info.html, last accessed at December 13th, 2019
12. 17 U.S. Code § 107. Limitations on exclusive rights: Fair use, https://www.law.cornell.edu/uscode/text/17/107, last accessed at December 13th, 2019
13. European Parliament & Council, Directive on the harmonisation of certain aspects of copyright and related rights in the information society (Information Society Directive)
14. Mark Zhou (Ed.), Education and Management, https://books.google.pt/books?id=6WOrCAAAQBAJ&printsec=frontcover&hl=pt-PT#v=onepage&q&f=false, last accessed at December 18th, 2019
15. Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC
16. Copyright | law, https://www.britannica.com/topic/copyright, last accessed at December 19th, 2019

A Survey of Android Attacks Detection Techniques

José Duarte

Lusofona University of Porto, Portugal
fernandoteixo_10@hotmail.com

Abstract. In this age of technology, mobile devices have become indispensable for humans. Most of these mobile devices have android operating system and as this number grows, the number of applications and malware, consequently also grows, which leads to greater concern and prevention, in this case, the android world. Many of these malicious applications are available on android's play store, making it an arduous task for the user to distinguish between which applications are clean. Somehow, there are several malware detection tools, which makes it difficult for malicious applications to penetrate, but malware writers use various techniques to avoid these tools. That said, this paper aims to explore the different attack detection techniques of Android and make some suggestions for defense mechanisms.

Keywords: Malware Detection, Android, Mobile Devices, Applications, Security, Android Attacks, Detection Techniques

1 Introduction

Nowadays, mobile devices are of great importance to humans, having exceeded the 5 billion mark, according to Hootsuite and We Are Social, accounting for a 67% share of the world's population [1]. These mobile devices are getting better technology at both chip design and microprocessor computing power levels, offering a wide range of features, and this is one of the reasons for their soaring popularity. Most users regard them as a reliable and private communication channel having access to various personal information. Within these mobile devices, there are several operating systems, but the most used is Android, with over 2 billion active devices [2]. It has become popular because of its low cost and because Android operating system code is made available by Google under open source license. By having such features and popularity, Android System-based devices inevitably attract the attention of cybercriminals who are creating and distributing malicious programs. According to Maya Horowitz (director of threat intelligence) and Check Point research, "The sharp rise in mobile banking malware is related to the growing use of mobile banking applications", as hackers are increasingly focused on theft of credentials, vigilance, and malicious advertising [3]. In many cases, malware attacks follow distribution strategies like those of desktop users, with applications running silently in the background, without the victim noticing. This article is organized as follows, section 2 addresses security challenges for mobile device users; Section 3 presents the Android security architecture; Section 4 presents the most popular malware types with a brief introduction. Section 5 discusses some malware

10.11228/dpsc.02.01.010

detection techniques; Section 6 presents a real case of a ransomware attack; and to finish we have the conclusion.

2 Security Challenges for Mobile Device Users

Mobile devices were created for the main purpose of communication, but nowadays these pocket computers can be used for various daily needs like searching for any information, making payments, entertainment and many other things, but this level of comfort has brought with it an extreme number of security risks to our personal information.

- Physical Security: Physical security is when the mobile device is lost or stolen. The personal data of the device user may be stolen and misused.
- Insecure Data Storage: Insecure data storage is the most common problem, found in 76% of mobile applications [4], so access to personal data such as name, address, date of birth, bank information, family photos, social network, email address, as well as access to work information (company name, job title and the like). Hackers do not need physical access to a mobile device to steal data as 89% of vulnerabilities could be exploited using malware [4]. Most cases are caused by deficiencies in application security mechanisms, but cyber-attacks also depend on user inattention leading to financial losses for users.
- Mobile Browsing: Normally, on mobile devices it is not possible to see the entire URL or web address, so it is difficult to prevent us from a phishing attack, for example.
- Multiple User Logging: There is a progressive growth in social media and single sign-on (SSO) as most mobile applications are insecure due to the possibility of allowing the user to access various services that require authentication by performing authentication only once. Hackers who gain access to login credentials for a website or application such as Facebook may also have access to a user's profile page.
- Client-Side Injection: The client-side injection results in the execution of malicious code on the client side, the mobile device and this through a mobile app. This malicious code is often provided in the form of data. What they target is the data on the device with SQL injection; the mobile user session with JavaScript injection (XSS, etc.), the application interfaces or functions, and the Binary Code itself.[5]
- Improper Session Handling: Many developers allow long user sessions that do not expire or use session tokens that are too predictable. They often do this because companies want users to have quick access to shopping and checkout so that sales are made immediately, and no second opinion is created. Long-term sessions invite vulnerabilities when performing financial tasks. Poor session management can provide clues about unauthorized access by hijacking sessions on mobile devices.[6][7]
- Weak Authentication and Brute Force Attack: Many applications rely on password-based authentication as a single factor, and often the owners of these applications do not enforce strong passwords and many users are exposed to a host of threats, including brute force attack. About 5% of confirmed data breach incidents in 2017 resulted from brute force attacks [8] and these attacks are simple and reliable as

attackers use computational power to perform their work by testing different username combinations and passwords until you find the key. [6]

3 Android Security Architecture

Android is an open source software platform for mobile devices. It includes a Linux Kernel, middleware framework, and core applications. The android has limited resource, so it’s very difficult to implement traditional security services. Therefore, researchers are trying to propose different behavioral approach to guard against malware.[9]

- Permission Mechanism: The purpose of a permission is to protect the privacy of an android user. Android applications must request permission to access user confidential data (such as contacts and SMS) and certain system features (such as camera and internet). A central design point of Android's security architecture is that no application, by default, can perform operations that would adversely impact other applications, the operating system, or the user. [10]
- Sandboxing: On the Android system each application is assigned a unique UserID. Android uses the UID to set up a kernel-level Application Sandbox. This isolates applications from each other by protecting them, for example, if application A attempts to do something malicious, such as reading application B's data without permission, will be prevented from doing so because it does not have the appropriate default user privileges. The sandbox is based on process separation and file permissions. [11]
- Access Control: In access control the mechanism of each archive has specific access rule and each process assigns a UserID. Each process has a specific permission to read, write or execute the file. [9]
- Components Encapsulation: Application components can be specified as public or private. Private components are accessible only by components within the same application. When declared public, components can also be accessed by other applications. However, full access can be limited by requiring calling ap-plications to have specified permissions. [9]
- Application Signing: Android uses cryptographic signatures to verify the origin of applications and establish trust relationships between them, so developers need to sign application code. This allows you to enable signature-based permissions or allow applications from the same source to share the same UserID. There is a certificate that is self-signed by the developer that is validated at application installation time. [9] [12]

4 Android Malware Attacks

Cybercriminals are increasingly focusing on mobile devices, with Android being the hardest hit due to its characteristics and this is because users ignore all or almost everything about mobile apps, or don't care about it. that favors cybercriminals. Therefore, additional security knowledge of mobile devices is required, as well as better security solutions and policies. To obtain confidential financial information, hackers have developed and spread mobile malware. Malware is software that has been coded to damage devices, harm users, and steal data by infecting the operating system without the user's knowledge or approval. Malware is often developed by hacking teams who are often just looking for a way to make money, either by proliferating their own malware or through auctioning on the Dark Web. This malicious software can be used as protest tools, to test the security of a network, or even as weapons of war between governments [15]. Mobile malware often steals information stored on users 'mobile devices or sends SMS to premium numbers for the hackers' monetary profit. Stolen information may include International Mobile Equipment Identity (IMEI) numbers, International Mobile Subscriber Identity (IMSI) numbers, Sub-scriber Identity Module (SIM) serial number, user credentials for future misuse, contacts or location of the Global Positioning System (GPS). Some mobile malware turns the infected phone into a bot that can be remotely controlled by the Command and Conquer (C&C) server. [13]

4.1 Types of Malware on Android

There are several types of malware, all with different forms of penetration and their list is far from defined, but some of the best known are:

- Virus: Viruses are a piece of code that replicates and is dispatched by the application, so they attach themselves to clean files and infect other clean files. They can spread uncontrollably, damaging a system's core functions and deleting or corrupting files, but they are also used to deceive information and steal money. They usually appear as an executable file (.exe). The most popular examples of viruses on Android are: Universal Cross-Site Scripting Attack (UXSS), Malware Hidden in Downloaded Applications, Lasco, Command & Control (C & C), Card-Block, CardTrap Android Installer Hijacking and Crossover. [13]
- Worms: Worm can replicate and disperse across devices to devices without any user interaction to perform. Worms infect entire device networks, either locally or over the internet using network interfaces. They use each infected machine to infect more others. They are usually received by SMS, MMS or another digital me-dia. The most popular example of the worm on android is the ADB.Miner An-droid. [13]
- Trojan: This type of malware pretends to be a legitimate program or hides in an original program that has been breached. They need to be installed by the user unlike worms. Once installed, Trojans can steal passwords, disable certain apps or lock the mobile device for a certain period. The most popular examples of Trojan are MasterKey, Fake-Player, GantSpy, DownAPK, etc. [13] [15][16]
- Spyware: This is malware designed to spy. It hides in the background and records online activities including passwords, credit card numbers, browsing routine and more. Exploiting vulnerabilities is the most important Spyware import goal. An example of spyware on Android is RedDrop. [13][15] [17].
- Ransomware: This malware is used to lock the device, and to unlock a payment is required to access your data. After payment the malware disappears. The most

popular ransomware Android malware is Xbot, Simpllocker FakeDefender [18] and adultPlayer. [13] [15]

- Botnets: Botnets often use special trojans to breach the security of mobile devic-es. The botnet is a piece of code used to "turn" a device into a bot without the user's consent, then these bots are all connected and thus form a "bot-network" or "botnet". Its purpose is to collect information. The best-known botnets in the Android operating system are Geinimi, Beanboot and DoubleDoor. [13] [18] [43]
- Rootkit: Rootkit is software designed to hide or conceal the existence of certain normal detection methods or processes, Rootkit also has administrative access to run various malicious applications to steal harmful action information and edit the configuration of the rootkit. system. There are some examples of Rootkit malware, but the most popular on Android are Godless, HummingBad, and Checkpoint. [13] [19]
- Backdoor: Backdoor is used to open any port for other applications and is a method that both authorized and unauthorized users can bypass normal security measures and gain high-level access to a computer system, network, or software application. When malicious as by unauthorized users becomes very dangerous malware. Brador is very popular backdoor malware. [13] [20]
- Keylogger: Keyloggers are applications that, once installed on a system, run to monitor all keypad entries. Then you can consult everything that was typed. The most common Malware Key-Logger on Android is FlexiSpy, mSpy. [13] [21]

5 Malware Detection Techniques

Malware in the android operating system is increasing day by day, which leads to a greater need to detect it to make it more secure. Very often mobile devices exhibit abnormal behavior that is driven by malicious malware that can harm the user in very dangerous ways, such as sending the user's private information to an unknown server. The techniques used to detect malware can be broadly categorized into two categories which are Anomaly-based detection and Signature-based detection. In fig.1 is represented the structure.

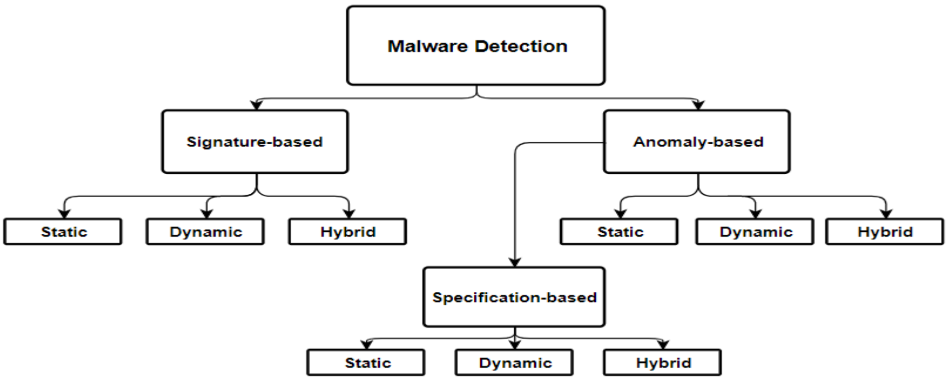


Fig. 1. A classification of malware detection techniques.[21]

5.1 Anomaly-based detection

This technique uses your knowledge of what constitutes normal behavior to decide whether the program under inspection is malware, tracking different parameters and the status of device components. Anomaly-based detection usually needs to work on a statistically significant number of packages, because any package is just an anomaly compared to some baselines. A special type of anomaly-based detection is called Specification-based detection. Specification-based techniques take advantage of some specifications or rulesets of what is valid behavior to decide whether the program under inspection is malware, programs that violate the specification are considered anomalous and generally malicious. [21] [22]

5.2 Signature-based detection

A signature is a sequence of bytes extracted from previously known malware, i.e. it uses the characterization of what is known as malicious to decide the maliciousness of a program under inspection, so if that pattern or signature is discovered again, the file may be marked as infected. This technique becomes a bit more limited as you always must access the signature database for regularly updating newly created signatures, but it offers higher malware detection accuracy. [21] [22]

5.3 The Comparison of different approaches for malware detection

Specific analysis of an anomaly or signature-based technique is determined by how the technique gathers information to detect malware. Each detection technique can employ one of three different approaches: static, dynamic or hybrid. A static approach attempts to detect malware before program execution under inspection; The dynamic approach attempts to detect malicious behavior during program execution or after program execution; The hybrid combines both ways, so static and dynamic information is used to detect malware. [21] [22]

A. Static Analysis: The static analysis deals with the features which are extracted from the application file without executing. The most popular dodging technique is known as Update Attack in which the malicious content is downloaded and installed as part of the update. This is not possible to detect by static analysis techniques. Permission and API calls are the most common features of static analysis as extracted from AndroidManifest.xml, thus can influence the malware detection rate to a high level studied by various researchers especially on meta-data available in Google Play Store.[23] Table 1 shows the advantages and disadvantages of static analysis.[21][24]

Advantages	Disadvantages
-It allows a complete analysis of a given; - It can cover all possible execution paths of a malware sample; - It is generally safer than dynamic approach as the source code is not actually executed.	-It is ineffective against previously unseen attacks and hence it cannot detect new and unknown intrusion methods as no signatures are available for such attacks. – The source code of malware samples is not readily available – It can be extremely timeconsuming and awkward process

Table 1. Advantages and Disadvantages of Static Analysis [22]

B. Dynamic Analysis: Dynamic analysis is a dynamic behavioral detection method that builds the operating environment using a sandbox, virtual machine, and so on, and simulates application execution to acquire the application behavior model. The goal is to find errors in a program while it is running, rather than repeatedly scanning offline code.[24] Table 2 presents some advantages and disadvantages of dynamic analysis.[21]

Advantages	Disadvantages
- It can avoid obfuscation issues, so it is easy to see the actual behavior of a program. - It can detect new intrusion method and can detect new malware	- The main drawback is that usually it monitors only one execution path, so it suffers from incomplete code coverage. - There is also the danger of harming third party systems, if the analysis environment is not properly isolated or restricted respectively. - Furthermore, malware samples may alter their behavior or stop executing at all once they detect to be executed within a controlled analysis environment.

Table 2. Advantages and Disadvantages of Dynamic Analysis [22]

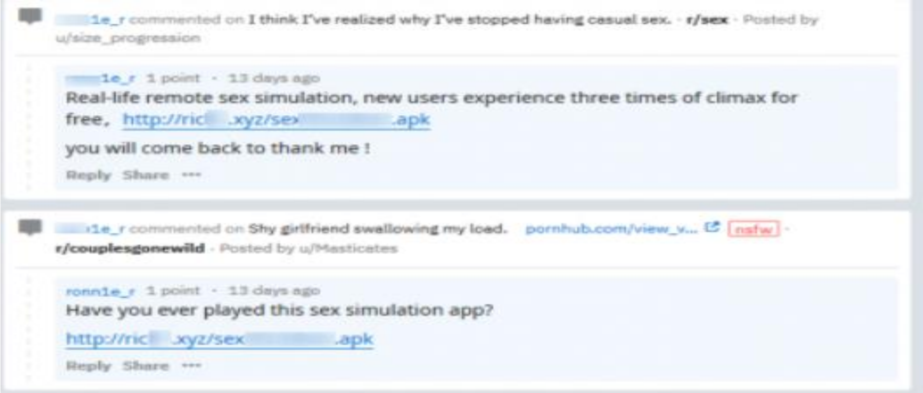
C. Hybrid Analysis: Hybrid analysis is a combination of static and dynamic analysis. It is a technology or method that can integrate runtime data extracted from dynamic analysis into a static analysis algorithm to detect malicious behavior or functionality in applications. The hybrid analysis method involves the combination of static resources obtained by analyzing the application and the dynamic resources and extracted information as the application runs. It uses advantages and reduces the disadvantages of both dynamic and static analysis. [22][21][24]

6 Real Case of Ransomware

A new ransomware has emerged which is propagated via SMS message, which was detected by ESET Mobile Security as Android / Filecoder.C. This new ransom-ware has been distributed through various online forums and affects An-droid versions 5.1 and up. It uses the victims contact list and thus propagates via maliciously linked SMS to all contacts listed on the device. Once the malicious SMS messages are sent, the threat encrypts most files on the user's device and requests a ransom.[26]

6.1 Distribution

This malware is distributed through attractions created by these attackers, for example, with pornography-related publications. In all comments or posts made (in this case on reddit), attackers included links or QR codes that were directed to malicious applications. In fig.2 an example is presented. [26]



[redacted]1e_r commented on I think I've realized why I've stopped having casual sex. · r/sex · Posted by u/size_progression

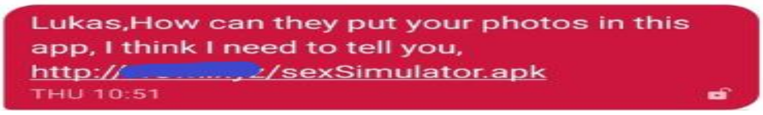
[redacted]1e_r 1 point · 13 days ago
Real-life remote sex simulation, new users experience three times of climax for free, http://ric[redacted].xyz/sex[redacted].apk
you will come back to thank me !

[redacted]1e_r commented on Shy girlfriend swallowing my load. pornhub.com/view_v... nsfw · r/couplesgonewild · Posted by u/Masticates

ronnie_r 1 point · 13 days ago
Have you ever played this sex simulation app?
http://ric[redacted].xyz/sex[redacted].apk

Fig. 2. Comments made on Reddit [26]

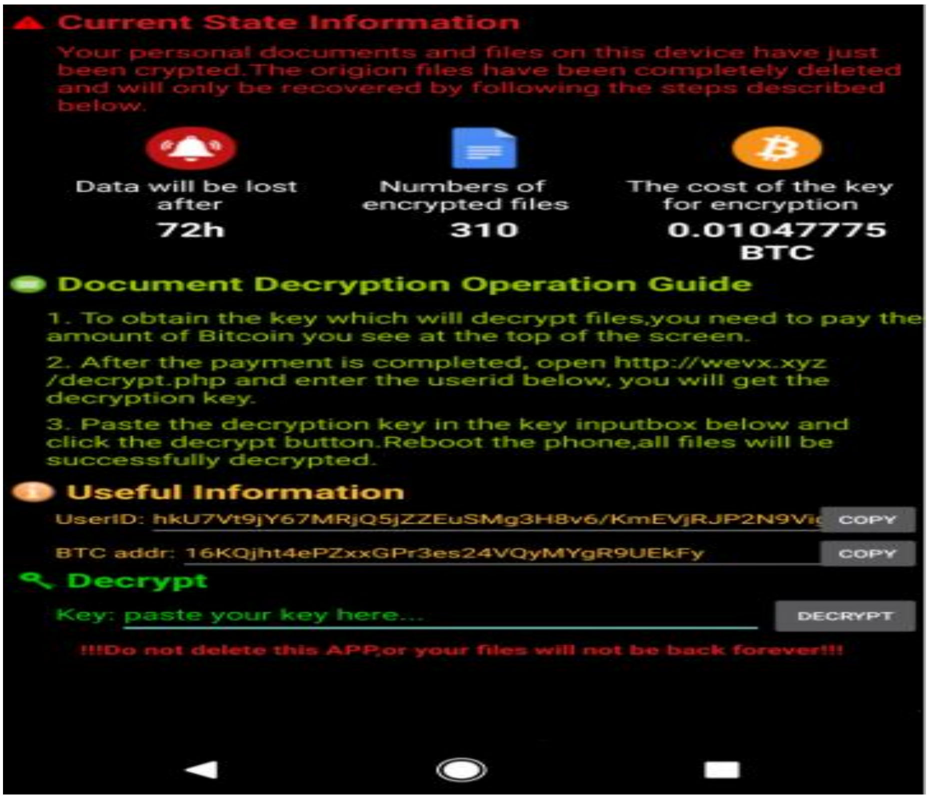
The Android / Filecoder.C ransomware to increase credibility, presents a link depending on the theme that is created as bait. In fig. 3 is an example of a link that appears as if it belonged to an application that allegedly uses the victim's photos. To maximize range ransomware has a model of the same message in several different languages. Before the message is sent, the threat chooses the version that matches the victim's device's language setting.[26]



Lukas,How can they put your photos in this app, I think I need to tell you, http://[redacted]/sexSimulator.apk
THU 10:51

Fig. 3. An SMS with a link to the ransomware.[26]

After the victims receive the SMS message with the link to the malicious application, it must be installed manually. After the application starts, as promised in the reddit comments, it shows an online simulation game, in this sexual case, but the main goal is to communicate with C&C (command & control), propagating messages. malicious and implementing the encryption / decryption mechanism. Ransomware can send text messages because it has access to the user's contact list. The ransomware then passes through files located in accessible storage and encrypts most of them. After encrypting the files, ransomware displays your ransom note, as shown in Figure 4. [26]



Current State Information

Your personal documents and files on this device have just been crypted.The origion files have been completely deleted and will only be recovered by following the steps described below.

Data will be lost after	Numbers of encrypted files	The cost of the key for encryption
72h	310	0.01047775 BTC

Document Decryption Operation Guide

1. To obtain the key which will decrypt files,you need to pay the amount of Bitcoin you see at the top of the screen.

2. After the payment is completed, open http://wevx.xyz /decrypt.php and enter the userid below, you will get the decryption key.

3. Paste the decryption key in the key inputbox below and click the decrypt button.Reboot the phone,all files will be successfully decrypted.

Useful Information

UserID: hkU7Vt9jY67MRjQ5jZZEuSMg3H8v6/KmEVjRJP2N9Vi

BTC addr: 16KQjht4ePZxxGPr3es24VQyMYgR9UEkFy

Decrypt

Key: paste your key here...

!!!Do not delete this APP,or your files will not be back forever!!!

Fig. 4. Rescue message presented by the Android/Filecoder.C. [26]

6.2 File Encryption Engine

Ransomware uses asymmetric and symmetric encryption, generating a public and private key pair. The private key is encrypted using the RSA algorithm with the hard-coded value stored in the code and sent to the attacker's server. To encrypt the files, ransomware generates a new AES key for each file that will be encrypted. This AES key is encrypted using the public key and is placed before each encrypted file, resulting in the following pattern: "((AES) public key + (File) AES). seven ", Fig. 5 illustrates in a more exemplary manner the above pattern. [26]

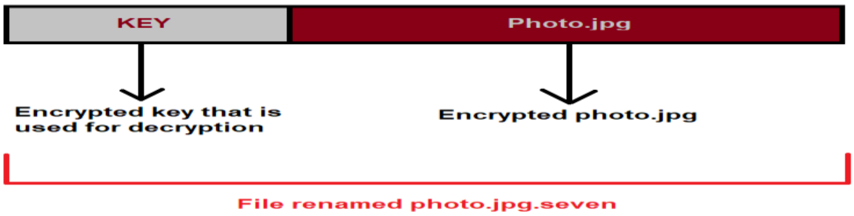
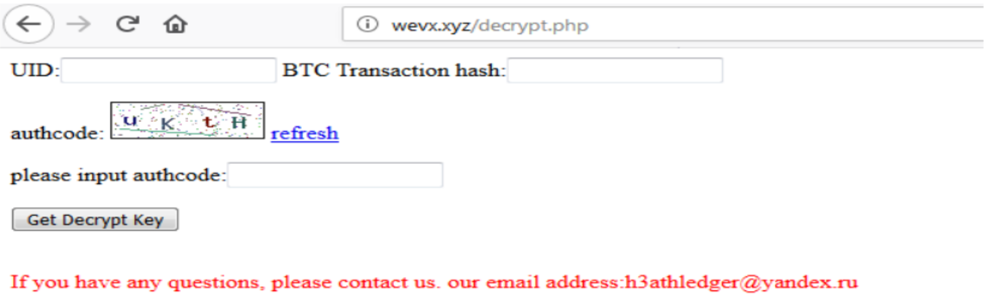

KEY
Photo.jpg
Encrypted key that is used for decryption
Encrypted photo.jpg
File renamed photo.jpg.seven

Fig. 5. Overview of the structure of encrypted files.[26]

6.3 Decryption Engine

The code to decrypt encrypted files is present in ransom-ware. If the victim pays for the ransom, the ransomware operator can verify it through the website shown in Figure 6 and send the private key to decrypt the files. [26]



If you have any questions, please contact us. our email address:h3athledger@yandex.ru

Fig. 6. Redemption payment verification web page.[26]

6.4 How to be protected

There are a few ways to prevent these attacks, which every user should do, which are: to keep devices up to date; download apps only through official stores; Before installing any app, check its rating and comments; Verify the permissions requested by the application; and use a mobile security solution.[26]

7 Conclusion

Most users think that mobile devices are a 100% safe device, or that only malicious cases happen to others, but it is not the best way to think when we talk about technology.

In this article, some security challenges for mobile users have been described, as a secure or informed user is much harder to fool than the uninformed one. Also introduced was the Android architecture, which is the system most subject to vulnerabilities derived from its features, not to mention that increasingly there are mobile banking applications that also catch the attention of hackers. The main point of this paper is presented in section 5, which analyzes the most well-known detection techniques, namely Signature Based Detection and Anomaly Based Detection, which are divided into 3 types which are static, dynamic and hybrid, based on detection. in anomaly a special type that is Specification Based Detection. We hope that with this article mobile users will get more information to be properly informed about possible attacks, and not an easy target to deceive, such as the real case of ransomware (section 6)

References

1. Tecmundo, https://www.tecmundo.com.br/celular/117849-5-bilhoes-pessoas-usam-celular-mundo-pesquisa.htm, [Last visited (20/11/2019)]
2. Tecmundo,https://www.tecmundo.com.br/dispositivos-moveis/141038-android-tem-2-5-bilhoes-usuarios.htm, [Last visited (20/11/2019)]
3. Zdnet, https://www.zdnet.com/article/mobile-malware-attacks-are-booming-in-2019-these-are-the-most-common-threats/, [Last visited (20/11/2019)]
4. Positive Technology, https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/, [Last visited (22/11/2019)]
5. Appknox,https://www.appknox.com/blog/understanding-owasp-top-10-mobile-client-side-injection, [Last visited (22/11/2019)]
6. Khan, J., Abbas, H., & Al-Muhtadi, J. Survey on mobile user's data privacy threats and defense mechanisms. Procedia Computer Science, 56, 376-383, (2015).
7. Appknox, https://www.appknox.com/blog/understanding-owasp-top-10-mobile-improper-session-handling, [Last visited (22/11/2019)]
8. Varonis, https://www.varonis.com/blog/brute-force-attack/, [Last visited (23/11/2019)]
9. Hur, J. B., & Shamsi, J. A. A survey on security issues, vulnerabilities and attacks in Android based smartphone. In International Conference on Information and Communication Technologies (ICICT) (pp. 40-46), (2017, December).
10. Android Developers, https://developer.android.com/guide/topics/permissions/overview, [Last visited (27/11/2019)]
11. Android Open Source Project, https://source.android.com/security/app-sandbox, [Last visited (27/11/2019)]
12. Davi, Lucas, Alexandra Dmitrienko, Ahmad-Reza Sadeghi, and Marcel Winandy. "Privilege escalation attacks on android." In International Conference on Information Security, pp.346-360, (2010).
13. Khan, M.; Tripathi, R.; Kumar,A.; “A Malicious Attack and Defense Techniques on Android-Based Smartphone Platform”, Internation Journal of Innovative Technol-ogy and Exploring Engineering (IJITEE), Volume 8, Issue-8S3, (2019, June)
14. AVG, https://www.avg.com/pt/signal/what-is-malware, [Last visited (29/11/2019)]
15. Avast Blog, https://blog.avast.com/pt-br/como-detectar-e-remover-um-virus-do-seu-telefone-android, [Last visited (06/12/2019)]
16. Tecmundo, https://www.tecmundo.com.br/seguranca/196-o-que-e-um-trojan-.htm, [Last visited (06/12/2019)]

17. TechTudo, https://www.techtudo.com.br/noticias/2019/07/o-que-e-spyware-entenda-como-age-o-app-espiao-e-veja-como-se-proteger.ghtml, [Last visited (10/12/2019)]
18. Symantec, https://www.symantec.com/connect/blogs/simplocker-first-confirmed-file-encrypting-ransomware-android, [Last visited (12/12/2019)]
19. Canaltech, https://canaltech.com.br/seguranca/O-que-e-rootkit/, [Last visited (13/12/2019)]
20. Malwarebyte, https://www.malwarebytes.com/backdoor/, [Last visited (13/12/2019)]
21. Idika, N., & Mathur, A. P. A survey of malware detection techniques. Purdue University, 48, 2007-2, (2007).
22. Baraiya, D., & Diwanji, H. A Survey on Android Malware and Malware Detection Techniques, pp.47-53, (2016).
23. RIASAT, R., SAKEENA, M., Chong, W. A. N. G., SADIQ, A. H., & WANG, Y. J. A Survey on Android Malware Detection Techniques. DEStech Transactions on Computer Science and Engineering, (2016).
24. Rao, V., & Hande, K. A comparative study of static, dynamic and hybrid analysis techniques for android malware detection. Int. J. Eng. Dev. Res (IJEDR), 5,pp.1433-1436, (2017).
25. Avg, https://www.avg.com/pt/signal/what-is-malware, [Last visited (29/11/2019)]
26. Welivesecurity,https://www.welivesecurity.com/br/2019/08/02/novo-ransomware-para-android-e-propagado-via-mensagens-sms/, [Last visited (19/12/2019)]

Android Attacks Detection Techniques

Hugo Marques

Lusófona University of Porto, Portugal
hugomaarqz@gmail.com

Abstract. Nowadays, almost everyone has a mobile device, especially a smartphone. Most people who have a smartphone are constantly at risk, often due to the applications they install, and just the fact that they connect to the internet for various purposes, they get unprotected from malware attacks, even though technology is becoming increasingly advanced. It is true that there are several malware detection tools, which are extremely important on every mobile device to protect each user's personal data. But it's also true that these tools just work to a certain point, and the "intruders" can get around these tools through numerous techniques. This study summarizes the various malware detection techniques used in the Android OS, explaining the advantages and disadvantages of each.

Keywords: Malware Attacks, Detection Tools, Personal Data, Android, Security, Application, Signature

1 Introduction

With the increased use of Android smartphones [1], the amount of android malware attacks is growing very quickly, and this growth brings several associated problems because it catches the attention of major malware attacks. Android is an opensource system unlike iOS, which is a closed system where apps are constantly inspected by security experts, so it makes the first system more vulnerable to external attacks.
These attacks are increasingly in 2019, and according to the information collected, researchers at Check Point examined cyberattacks in the first half of 2019 and found that those targeting smartphones and other mobile devices have risen by 50% compared with last year. The findings have been outlined in the Cyber Attack Trends: 2019 Mid-Year Report and the report suggests one of the key reasons for the sharp rise is the increased use of homebanking applications. This has seen cybercriminals following the money and increasingly distributing malware designed to steal payment data, login credentials, and ultimately funds from victims' bank accounts. In many cases, the malware attacks follow similar distribution strategies to those targeting desktop users, with the applications silently running in the background without the victim being any the wiser [2]. Android is the most popular platform for smart-phone based malware authors and sometimes even trusted applications can leak user's location and phone's identity and share it without its consent. These days we must be very updated and informed in order to keep up with what we can be struck with, so it is very important to know what android attacks are, how to spot a potential one and protect ourselves.

10.11228/dpsc.02.01.011

This paper focuses on describing mobile-based android attacks and its counter detection techniques. It's going to be analyzed the android security enhancement, what are the vulnerabilities and how Google's providing tools to protect users.

2 Android Environment: Attacks and Types of Malware

A malware attack is a type of cyberattack in which malware or malicious software performs activities on the victim's computer system, usually without his/her knowledge. [3]. Malware attacks can occur on all sorts of devices and operating systems, including Microsoft Windows, macOS, Android, and iOS. At least one type of malware attack is growing. Mobile ransomware attacks increased by a third in 2018 from the previous year. Most of those attacks occurred in the United States [4].

2.1 Types of Attacks on Android

The entire development lifecycle of Android has been subject to a rigorous security program, but it doesn't invalidate that android is vulnerable to cyber-attacks and there are several cyber-attacks which cause lot of harm to users. These attacks can be isolated cyber-attacks or based upon use of malware as attack tool. Beyond that we can observe clearly that Android developers are keep improving the Android version by version, but in the other hand that shows that the older android versions had some security issues and vulnerabilities and that leads to malware and cyber-attacks. Patching these vulnerabilities prevents some attacks but there are always others which attackers discovers and forms attacks around these vulnerabilities.

Attack type	MALWARE	Description	Impact
Data theft	SMS/Email	The users get a SMS or a email giving them big bounties with a link. When they click that they may be redirected to a malicious website giving away their sensitive information or may lead to financial loss.	The most innocent people can be fooled by these messages and their personal information is exposed.
Identity Theft	NFC/OTP	Attacker gets access of mobile device and impersonate the user using their smartphone running Android.	Loss can be very huge and only limited with the attacker though
Bloat-ware	Adware	Nasty form of bloatware that exists to pump ads to the user, via websites or via popups that come up directly on computer screen.	Adware can slow PC down - it can spy on user as well or expose user's system to other dangers.

Table 1. Types of Android attacks [5]

2.2 Types of Malware

Trojans: A Trojan, often mistakenly thought of as a virus or a worm, is a malicious program that enters in a device, hidden in programs that seem harmless. It serves to open a door so that malicious users can break into a person's computer or device. A Trojan is a program that simulates some useful functionality that can harm computers and their users, such as hacking or stealing user passwords. Their main propagation is through the Internet, where they are offered as tools with useful - or even vital - functions for devices**.** The two most common types of Trojans are Keyloggers (which are commonly used to steal passwords) and Backdoors (files that allow door openings for intrusion) [6].

Worm: Worms is a type of malware that spreads copies of itself from computer to computer. A worm can replicate itself without any human interaction, and it does not need to attach itself to a software program in order to cause damage. Worms can be transmitted via software vulnerabilities. Or computer worms could arrive as attachments in spam emails or instant messages (IMs). Once opened, these files could provide a link to a malicious website or automatically download the computer worm. Once it's installed, the worm silently goes to work and infects the machine without the user's knowledge [7].

Adware: Adware is an unwanted software designed to cause advertisement to appear on the screen, mostly within a browser. Usually it uses a discrete method to disguise itself as legitimate or it infiltrates in another program to trick the users into installing it on PCs, tablets or mobile devices [8].

Ransomware: A Ransomware is a type of malware that prevents users from accessing your system or personal files and requires them to pay a ransom to return the access. Those files are still on the device, but the malware has encrypted the device, making the data stored on computer or mobile device inaccessible. That malicious software comes in several different forms. The two most common variations are Crypto ransomware and Locker ransomware.[9]

Rootkit: A rootkit is a clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence. The term rootkit is a connection of the two words "root" and "kit." Originally, a rootkit was a collection of tools that enabled administrator-level access to a computer or network. Root refers to the Admin account on Unix and Linux systems, and kit refers to the software components that implement the tool. Today rootkits are generally associated with malware – such as Trojans, worms, viruses – that conceal their existence and actions from users and other system processes [10].

Botnet: A botnet is a network of malware-infected computers that can be wholly controlled by a single command and control center operated by a threat actor. The network itself, which can be composed of thousands if not hundreds of thousands of computers, is then used to further spread the malware and increase the size of the network. [11] What happens is that botnets gain access to your machine through some piece of malicious coding. In some cases, your machine is directly hacked, while other times what is known as a "spider" (a program that crawls the Internet looking for holes in security to exploit) does the hacking automatically. [12]

2.3 Android Banking Malware: A Real Case of an Attack

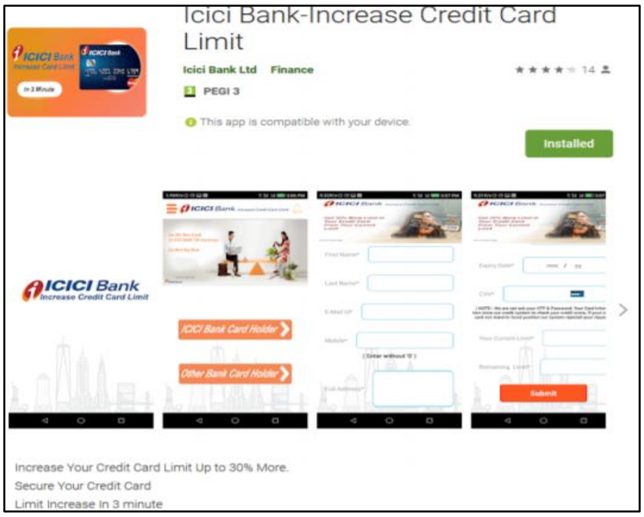
The most prevalent type of Android banking malware is the fake banking apps, in this paper it will be explored the impact of that approach on potencial victims. Malware in both these categories is designed to achieve the same goal: steal credentials for, or money from, their victims. Malware in both these categories is designed to achieve the same goal: steal credentials for, or money from, their victims' bank accounts. To achieve that, both sophisticated banking Trojans and fake banking apps need to elicit sensitive banking information from their victims and, if direct theft is the aim typically also need to gain access to SMS messages received on the compromised devices. To lure the valuable information from potential victims, both types of malware make use of phishing and bogus login forms. However, despite the similarities in their objectives, sophisticated banking Trojans and fake banking apps differ significantly in their strategy for deceiving victims. The following section will explore that difference and offer a more detailed look into the modus operandi of each distinct malware type [13].

Key features and strategy: Fake banking apps bet everything on the success of impersonation – their whole operation stands or falls on how believably they can imitate a legitimate banking application, or stand in for a non-existent one, from the very first moment a potential victim comes across them, up to the point when the victim enters sensitive information. Their weapon of choice is therefore their presentation – from app name, through app description, to icon and preview images, the apps need to appear trustworthy to attract unsuspecting users [13].

Modus operandi: To reach their malicious goals, fake banking apps typically take the following steps: 1) Trick victims into installing malware by posing as a legitimate banking app; 2) Obtain needed permissions; 3) Upon launch, display a phishing screen mimicking a legitimate banking app and requesting login credentials or credit/debit card details; 4) Harvest credentials or credit/debit card details entered into the bogus form; 5) Display an error/thank-you message; offer no further functionality; 6) Optional: Use SMS permissions to intercept one-time password (OTP); 7) Carry out fraudulent transactions using the victim's account or sell credentials on the black market; [13]

Distribution: Fake banking apps are often spread across Google Play or unofficial app stores, where they represent legitimate banking apps or other financial apps. Attackers who spread these malicious counterfeits try to lure their victims by using legitimate-looking application [13].

Targeting: Fake banking applications often focus on targeting customers from just one financial institution or service - the one they practice. In choosing their destination, some malware authors take advantage of the absence of an official mobile app for the destination bank or service, while others try to mislead users by impersonating existing official applications. Occasionally, counterfeits are intended to offer additional and compelling functionality to existing legitimate applications, such as bank rewards or offers to increase credit card limits (Figure 1) [13].



Icici Bank-Increase Credit Card Limit

Icici Bank Ltd Finance

PEGI 3

This app is compatible with your device.

Increase Your Credit Card Limit Up to 30% More.
Secure Your Credit Card
Limit Increase In 3 minute

Fig. 1. Malicious app impersonating Indian Icici bank and claiming to increase credit card limit for its customers [13]

Functionality and permissions: These apps functionality come down to displaying bogus login screens and harvesting credentials entered into the fake forms. After the credentials are stolen, some apps display generic messages with a promise to get back to the victim, as a cover for not offering any real functionality. Optionally, depending on permissions gained during and after installation, fake banking apps can also intercept and redirect SMS messages to bypass SMS-based 2-factor authentication. As users install these apps believing they are installing real banking applications, they are likely to grant the apps SMS permissions without thinking twice about it [13].

2.4 Google Services for Android Security

Google try to give extra security to Android devices and protect users by offering various services like Google Play Protect, which provides high security for users in many ways.

Data Protection: Google Play keep apps and data safe [14].

Scanning: Every day, it automatically scans all the apps on Android phones and works to prevent harmful apps from ever reaching them. This tool checks all app developers on Google play, so even before downloading an app, the user knows that it has been verified and approved [14].

SafetyNet: Offers a set of services and APIs that help protect an app from security threats, including device tampering, incorrect URLs, potentially harmful apps, and fake users. There are four types of SafetyNet that will be presented next.

SafetyNet Attestation: Provides services for determining if a device running your app satisfies Android compatibility tests [15].

SafetyNet Safe Browsing: Offers services to determine if a URL has been marked as a known threat by Google [15].

SafetyNet reCAPTCHA: Protects apps against malicious traffic [15].

SafetyNet Verify Apps: Protects the devices against potentially harmful apps [15].

3 Malware Attacks Techniques

Attack Targeting and Inception: Cybercriminals will determine the method of initiating your attack. If profit is the primary objective, such as ransomware attacks, attackers will attack as many users as possible using spear-phishing attacks, in which recipients are urged to open the message attachment, which launches the malware program. Other comprehensive targeting methods involve using sites where attacks start through hidden redirects and drive-by-downloads. Attackers typically prefer public websites that run vulnerable web or application servers that they can take advantage of. Attacks targeting specific individuals can also leverage exploits and different types of social engineering techniques to entice an insider to inadvertently install malware inside an organization's firewall [16].

Exploit Discovery: Many attackers favor packaging malware into exploit kits that they covertly place on legitimate websites or host the malware on a fake website designed to look like a legitimate site. When a potential victim's browser connects with a website hosting an exploit kit, the kit probes the visitor's system and extracts information like OS version, browser type, and installed applications, in order to find vulnerabilities to exploit. Exploits and malware go hand in hand. All types of enterprise and consumer applications have vulnerabilities that can potentially be exploited, paving the way for malicious programs to find their targets. [16]

Payload Delivery: The malicious program will download and install a "payload" to the target endpoint device. This payload could be the piece of malware itself, or it could be a hidden downloader which then creates a backdoor through which multiple types of malware can be downloaded, allowing different attacks to be executed. [16]

Execution of Attack: The malicious program has reached its target and begins to run on the system, carrying out the attacker's intent. In the case of ransomware, the program will begin to encrypt the user's files or block critical system operations, thus locking the user out. More sophisticated attack code can be designed to trigger off of specific system events, or stealthily steal data over an extended period of time [16].

Malware Propagation: If a malware attack goes undetected or unmitigated, it will likely spread laterally, infecting other endpoints or even launching further targeted attacks via the network. As the malware persists, it communicates back to the attacker's back end, or to other command & control servers. Lateral spread is often the goal of attacks leveraging RATs (Remote Access Trojans). RATs are malware programs designed to establish administrative control over the host computer through back doors. Once such control is gained by an attacker, they can distribute RATs to other vulnerable computers on the network, establishing a botnet [16].

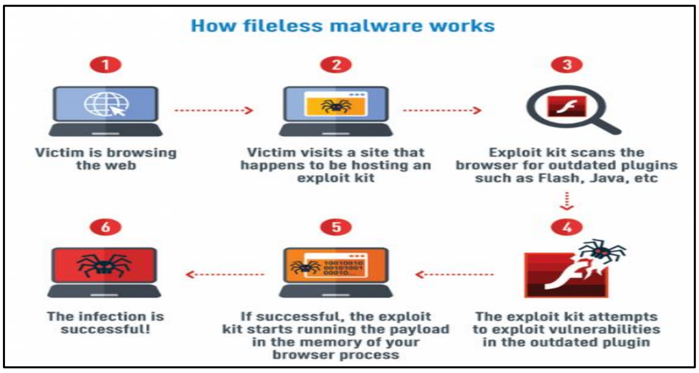

How fileless malware works
1
Victim is browsing the web
2
Victim visits a site that happens to be hosting an exploit kit
3
Exploit kit scans the browser for outdated plugins such as Flash, Java, etc
4
The exploit kit attempts to exploit vulnerabilities in the outdated plugin
5
If successful, the exploit kit starts running the payload in the memory of your browser process
6
The infection is successful!

Fig. 2. Spreading process of a malware [17]

4 Malware Detection Techniques

In this section will be analyzed the types of android malware detection techniques that exist. That techniques can be categorized in three main groups: 1) Signature-based detection, 2) Anomaly-based detection and 3) Specification-based detection. These three based detection tools can also be group on the based-on type of analysis static, hybrid or dynamic analysis. Static analysis is done without running an application while dynamic analysis deals with features that were extracted from the application while running. The following explains the analysis of these techniques more deeply.

Signature-Based Detection: Signature-based detection is a process where a unique identifier is established about a known threat so that the threat can be identified in the future. In the case of a virus scanner, it may be a unique pattern of code that attaches to a file, or it may be as simple as the hash of a known bad file. If that specific pattern, or signature, is discovered again, the file can be flagged as being infected. Suspected files are typically quarantined and/or encrypted in order to render them inoperable and useless. Clearly there will always be new and emerging viruses with their own unique code signatures, so the library of known code signatures is updated by the anti-virus software provider and if a new viral signature is detected, the updates are pushed out to users immediately and zero-day vulnerabilities are avoided [18][19][20].

ADVANTAGES	DISADVANTAGES
They are very efficient to detect without generating a large number of false alarms.	These types of detectors can only detect known attacks, which are included in the signature set that IDS has, so we must always be updating this set.
They can diagnose the use of a specific attack tool or technique.	Most of these detectors have very specific signatures, not detecting variants of the same attack.

Table 2. Advantages and disadvantages of Signature-based detection [23].

Anomaly-Based detection(behavior-based): Anomaly based analysis is based on watching the behavior of the device by keeping track of different parameters and the status of the components of the device. A key advantage of anomaly-based detection is its ability to detect zero-day attacks Anomaly-based detection generally needs to work on a statistically significant number of packets, because any packet is only an anomaly compared to some baseline. This need for a baseline presents several difficulties. For one, anomaly-based detection will not be able to detect attacks that can be executed with a few or even a single packet. While signature-based detection compares behavior to rules, anomaly-based detection compares behavior to profiles. These profiles still need to define what is normal, like rules need to be defined. However, anomaly-based profiles are more like white lists, because the profile detects when behavior goes outside an acceptable range. This analysis can be static, dynamic or hybrid [20][21][22].

ADVANTAGES	DISADVANTAGES
Detect usually behaviour and thus have the ability to detect symptoms of attacks without specific knowledge of details.	Usually produces a large number of false alarms due to the unpredictable behaviors of users and networks..
Can produce information that can be used to define signatures for misuse detectors	Often require extensive "training sets" of system event records in order to characterize normal behavior patterns.

Table 3. Advantages and disadvantages of Anomaly-based detection [23]

Specification-Based Detection: Specification-Based Detection is the derivate of anomaly- based detection and is much more complex than the others detection techniques cause its analysis can be performed at the layers below the Internet Protocol stack application layer or at the operating system control level. In specification-based system there exists a training phase which attempts to learn the all valid behaviour of a program or system which needs to inspect. The main limitation of specification-based system is that it if very difficult to accurately specify the behaviour the system or program. One such tool is Panorama which captures the system wide information flow of the program under inspection over a system and checks the behaviour against a valid set of rules to detect malicious activity. Specification based detection makes use of certain rule set of what is considered as normal in order to decide the maliciousness of the program violating the predefined rule set. Thus, programs violating the rule set are considered as malicious program. This type of detection is considered lower level. This analysis can be static, hybrid or dynamic too [20][21][22].

All malware scanners, essentially, utilize signature and anomaly -based techniques for perceiving personalities of programs.

a) Dynamic methods: Dynamic analysis is the testing and evaluation of a program by executing data in real-time. The objective is to find errors in a program while it is running, rather than by repeatedly examining the code offline. It is a detection technique which aims at evaluating malware by executing the application and the main advantage of this technique is that determines the application behavior during runtime and loads target data. The resource consumption in this analysis technique is more as compared to static analysis. Dynamic behavioral detection method constructs operation environment by using a sandbox, virtual machine, and other forms, and simulates the execution of the application to acquire the application's behavior model [24].

b) Static methods: In the static analysis, the analysis of the applications is done, and the features are extracted without executing the application on an emulator or device. In comparison to other analysis techniques for android malware detection, static analysis consumes fewer resources and time as it does not involve execution of the application. The major disadvantage of this analysis is code obfuscation because of which detecting the malicious behavior of the application becomes difficult as pattern matching is not possible. This analysis can detect runtime errors, logical inconsistencies, and possible security violations. The most commonly used static features are the Permission and API calls [24].

c) Hybrid methods: Hybrid Analysis is a combination of static and dynamic analysis. It is a technology or method that can integrate run-time data extracted from dynamic analysis into a static analysis algorithm to detect behavior or malicious functionality in the applications. The hybrid analysis method involves combining static features obtained while analyzing the application and dynamic features and information extracted while the application is executed. Though it could increase the accuracy of the detection rate, it makes the system cumbersome and the analysis process is time consuming. [24].

Factors	**Static Analysis**	**Dynamic Analysis**	**Hybrid Analysis**
Time required	Less	More	More
Input	Binary files, scripting language file etc.	Memory snapshots, runtime API data	Data obtained from both static and dynamic analysis
Code obfuscation	Yes	No	No
Resource Consumption (power & memory)	Less	More	More
Effectiveness and Accuracy	Less as compared to dynamic analysis	Better than static analysis	Better than static and dynamic analysis
Target code execution	Not possible	Possible	Possible
Advantages	Low cost and requires less time for analysis	Provides deep analysis and higher detection rate with unknown malware detection	Extracts features of static and dynamic analysis both, providing more accurate results
Limitations	Limited signature database and can detect only known malware types	More time and power consumption	High Cost

Table 4. Comparison between static, dynamic and hybrid analysis [24]

5 Conclusion

It’s so obvious that a good part of people is still outdated when we talk about technologies and the pros and cons of their advancements. People need to informate themselves about all what involves technology and not only about the “good part” of that. In this case we talk about a very known technology, the Android SO. The attacks on android by hackers are increasingly and the security remains compromised.
In this paper is presented all the android environment referring all the vulnerabilities despite the strict security program that Android has been subjected to. Within the Android Environment theme, is referred the 3 most known android attacks and what impact these produce. Are also mentioned the main types of malware and is chosen a real case of a malware attack. The way how Google provides her services to give extra security to Android devices and protect users is focused as well as the techniques of malware attacks, that is, how malware spreads and what are the stages until the end goal is reached. The main point of this paper in presented in point 4 where with searches done it was concluded that there are three main detection techniques which are all divided in static, dynamic or hybrid analysis.

To do this paper, was consulted many other selected papers of different authors to collect authentic information based on different knowledge. To resume I hope people get more informed about this subject to be more protected and prevented to these attacks.

References

1. Android tem mais de 2,5 bilhões de usuários, https://www.tecmundo.com.br/dispositivos-moveis/141038-android-tem-2-5-bilhoes-usuarios.htm, 2019/12/16
2. Mobile Malware attacks are booming in 2019: These are the most common threats, https://www.zdnet.com/article/mobile-malware-attacks-are-booming-in-2019-these-are-the-most-common-threats/, 2019/12/16
3. What is a Malware Attack, https://enterprise.comodo.com/what-is-a-malware-attack.php, 2019/12/16
4. Malware attacks: What you need to know, https://us.norton.com/internetsecurity-malware-malware-101-how-do-i-get-malware-complex-attacks.html, 2019/12/16
5. Khan, M.; Tripathi, R.; Kumar, A.; “A Malicious Attack and Defense Techniques on Android-Based Smartphone Platform”, International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume 8, Issue-8S3, June (2019)
6. Backdoor, https://www.malwarebytes.com/backdoor/, 2019/12/16
7. What is a computer worn, and how does it work, https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html, 2019/12/16
8. Adware, https://www.malwarebytes.com/adware/, 2019/12/16
9. Ransomware, https://www.malwarebytes.com/ransomware/, 2019/12/16
10. Rootkit: What is a Rootkit?, https://www.veracode.com/security/rootkit, 2019/12/16
11. What is a Botnet?, https://www.checkpoint.com/definitions/what-is-botnet/#, 2019/12/17

12. What is a Botnet", https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html, 2019/12/17
13. Štefanko, L.; "Android Banking Malware: Sophisticated trojans vs. Fake banking apps", ESET Malware Researcher, January (2019)
14. "Google Play Protect: Securing 2 billion users daily", "https://www.android.com/play-protect/", 2019/12/19
15. Protect against security threats with SafetyNet, https://developer.android.com/training/safetynet, 2019/12/19
16. Malware & Exploit Attacks Explained, https://newtecservices.com/malware-exploit-attacks-explained/, 2019/12/19
17. Fileless malware: Invisible threat or scaremongering hype, https://blog.emsisoft.com/en/29070/fileless-malware-attacks/, 2019/12/19
18. Limitations of Signature-Based Detection, https://bricata.com/blog/signature-detection-vs-network-behavior/, 2019/12/19
19. Sistema de Deteção de Intrusão – Artigo Revista infra Magazine 1, https://www.devmedia.com.br/sistema-de-deteccao-de-intrusao-artigo-revista-infra-magazine-1/20819, 2019/12/20
20. Sawle, P.; Gadicha, A.; Analysis of Malware Detection Techniques in Android, International Journal of Computer Science and Mobile Computing, Vol.3, Issue 3, March (2014)
21. Amro, B.; Malware Detection Techniques for Mobile Devices, International Journal of Mobile Network Communications & Telematics (IJMNCT) Vol.7, No.4/5/6, December (2017)
22. Mohata, V.; Dakhane, D.; Pardhi, R.; Mobile Malware Detection Techniques, International Journal of Computer Science & Engineering Technology (IJCSET), Vol 4, April (2013)
23. Cherrier, S.; Doudane, Y.; Fault-Recovery and Coherence in Internet of Things Choreographies, International Journal of Information Technologies and Systems Approach, Vol 10, Issue 2, December (2017)
24. Rao, V.; Hande, K.; A Comparative study of static, dynamic and hybrid analysis techniques for android malware detection, International Journal of Engineering Development and Research, Volume 5, Issue 2, (2017)

PAPERS IN ALPHABETICAL ORDER

A Survey of Android Attacks Detection Techniques......……………………. page 106

A Survey of Cyber Security Systems: Approaches for Attack Detection, Prediction and Prevention....………………………………………………..…............... page 21

A Survey of Cyber Security Systems: Approaches for Attack Detection, Prediction and Prevention........……………………………………………..…............... page 33

Analysis of Security in E-Commerce and M-Commerce.................................. page 74

Android Attacks Detection Techniques.......................………………..……. page 118

Information Privacy and Security on a Shared Resources Network: IP Spoofing Attacks...............……………………………………………………..…............... page 61

Major Challenges in Digital Contents Copyright Protection..………………….. page 86

Major Challenges in Digital Contents Copyright Protectional....………....….... page 96

Portugal Cyber threats Review: Targeted Health Institution.......…...............…. page 52

Review of cyber threats on Educational Institutions.......................…............... page 43

Web Applications Security Risk Quantification Based on Review of Past Six OWASP Top-10...............………………………………………………..…............... page 8

AUTHORS IN ALPHABETICAL ORDER

Amjad Zareen........ page 8

André Fontes........ page 86

David Pinto........ page 52

Hugo Barbosa........ page 21

Hugo Marques........ page 118

João Barreira........ page 96

Jorge Gonçalves........ page 21

Jorge Pinheiro........ page 43

José Duarte .... page 106

Mansoor Ahmed Khan........ page 8

Nuno Mata .... page 74

Pedro Graça........ page 61

Vera Oliveira........ page 33

Conference EOI :10.11228/dpsc
DPSC2020 Proceedings EOI: http://eoi.citefactor.org/10.11228/dpsc

PRIVACY AND SECURITY CONFERENCE 2020

PRIVACYANDSECURITYCONFERENCE.PT

UNIVERSIDADE LUSÓFONA DO PORTO