Universidad de Alcalá

Doctorado en Ingeniería de la Información y del Conocimiento

Departamento de Ciencias de la Computación

A Cybersecurity review of Healthcare Industry

Tesis Doctoral presentada por

CARLOS CILLERUELO RODRÍGUEZ

Directores:
Dr. José Javier Martínez Herráiz
Dr. Luis de Marcos Ortega

Alcalá de Henares, Octubre 2022

Dedication and acknowledgements

First of all I would like to express my sincere and deepest thanks my supervisors Dr. Luis de Marcos Ortega and Dr. José Javier Martínez Herraiz. Both of them have put their trust in me in numerous projects and also guided me through all my research period.

I would also like to acknowledge the support and funding for research provided by the European Commission. In a country where science is neither valued nor supported, the European Commission becomes one of the few realistic research funding options. It is a fact that this thesis would not be finished if Horizon2020 did not exist. I really hope that in the future we can have a country where science is supported and valued.

I must also give my special thanks and credits to my friend and research colleague Javier Junquera Sánchez. It is not a secret that Javier is a co-author on the majority of my scientific publications. That is because we shared numerous years of collaborative research work, failed projects and experiences. In some of my most difficult moments, Javier always have support me and led the research projects without doubts or complaints. This thesis would not have been written without Javier's work and support.

And last but not least I would like to thank my parents, Rosa and José. Without their support this thesis it would not have been finished in four years for sure.

—–BEGIN PGP MESSAGE—–
Version: GnuPG v1.2.9 (MingW32)

THVjaGUgY29udHJhIGV4dHJlbWlzbW8geSBlbCB0ZXJyb3IsIHBvciBsbyBjdWFsIHNlIG1lIHJlY29ub2
Npw7MgZWwgYmxhbmNvLiAKClJlY29ycsOtIGxvcyBjYW1pbm9zIGRlIEV1cm9wYSBjb24gcGFzacOzbiB5I
GdhbmFzLiAKClVuYSBlbmZlcm1lZGFkIG1lIGhpem8gdmVyIHN1ZnJpciB5IGRlc2FwYXJlY2VyIGEgYWx
ndW5hcyBkZSBtaXMgcGVyc29uYXMgbcOhcyBxdWVyaWRhcy4gCgpEb2N0b3JlcyBlIGluZ2VuaWVyb3Mg
YXBvc3Rhcm9uIHBvciBtw60gZW4gZWwgaG9yaXpvbnRlIGRlIEV1cm9wYS4gCgpQYXNlIGxvcyBtb21lbnR
vcyBtw6FzIGR1cm9zIGRlIG1pIHZpZGEgY29uIHVuYSBwZXJzb25hIHF1ZSBkZXNhcGFyZWNpw7MuIAoK
RHVyYW50ZSBtdWNobyB0aWVtcG8gbWkgcG9zZWNpw7NuIG3DoXMgcHJlY2lhZGEgZnVlIHVuYSBjdW
NoYXJhLgoKU2kgZXN0w6FzIGxleWVuZG8gZXN0byBxdWl6w6FzIGhheWEgb8OtZG8gaGFibGFyIGRlIG1
pLg

—–END PGP MESSAGE—–

Resumen

Antecedentes

La ciberseguridad no es un concepto nuevo de nuestros días. Desde los años 60 la ciberseguridad ha sido un ámbito de discusión e investigación [1]. Aunque los mecanismos de defensa en materia de seguridad han evolucionado, las capacidades del atacante también se han incrementado de igual o mayor manera. Prueba de este hecho es la precaria situación en materia de ciberseguridad de muchas empresas, que ha llevado a un incremento de ataques de ransomware [2][3] y el establecimiento de grandes organizaciones criminales dedicadas al cibercrimen [4][5]. Esta situación, evidencia la necesidad de avances e inversión en ciberseguridad en multitud de sectores, siendo especialmente relevante en la protección de infraestructuras críticas. Se conoce como infraestructuras críticas aquellas infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales [6]. Dentro de esta categorización se encuentran los servicios e infraestructuras sanitarias. Estas infraestructuras ofrecen un servicio, cuya interrupción conlleva graves consecuencias, como la pérdida de vidas humanas. Un ciberataque puede afectar a estos servicios sanitarios, llevando a su paralización total o parcial, como se ha visto en recientes incidentes [7][8][9], llevando incluso a la pérdida de vidas humanas [10]. Además, este tipo de servicios contienen multitud de información personal de carácter altamente sensible. Los datos médicos son un tipo de datos con alto valor en mercados ilegales, y por tanto objetivos de ataques centrados en su robo [11].

Por otra parte, se debe mencionar, que al igual que otros sectores, actualmente los servicios sanitarios se encuentran en un proceso de digitalización [12]. Esta evolución, ha obviado la ciberseguridad en la mayoría de sus desarrollos, contribuyendo al crecimiento y gravedad de los ataques previamente mencionados.

Metodología e investigación

El trabajo presentado en esta tesis sigue claramente un método experimental y deductivo. Está investigación se ha centrado en evaluar el estado de la ciberseguridad en infraestructuras sanitarias y proponer mejoras y mecanismos de detección de ciberataques. Las tres publicaciones científicas incluidas en esta tesis buscan dar soluciones y evaluar problemas actuales en el ámbito de las infraestructuras y sistemas sanitarios.

La primera publicación, 'Mobile malware detection using machine learning techniques', se centró en desarrollar nuevas técnicas de detección de amenazas basadas en el uso de tecnologías de inteligencia artificial y 'machine learning'. Esta investigación fue capaz de desarrollar un método de detección de aplicaciones potencialmente no deseadas y maliciosas en entornos móviles de tipo Android. Además, tanto en el diseño y creación se tuvo en cuenta las necesidades específicas de los entornos sanitarios. Buscando ofrecer una implantación sencilla y viable de acorde las necesidades de estos centros, obteniéndose resultados satisfactorios.

La segunda publicación, 'Interconnection Between Darknets', buscaba identificar y detectar robos y venta de datos médicos en darknets [13]. El desarrollo de esta investigación conllevó el descubrimiento y prueba de la interconexión entre distintas darknets. La búsqueda y el análisis de información en este tipo de redes permitió demostrar como distintas redes comparten información y referencias entre ellas. El análisis de una darknet implica la necesidad de analizar otras, para obtener una información más completa de la primera.

Finalmente, la última publicación, 'Security and privacy issues of data-over-sound technologies used in IoT healthcare devices' buscó investigar y evaluar la seguridad de dispositivos médicos IoT ('Internet of Things'). Para desarrollar esta investigación se adquirió un dispositivo médico, un electrocardiógrafo portable [14], actualmente en uso por diversos hospitales. Las pruebas realizadas sobre este dispositivo fueron capaces de descubrir múltiples fallos de ciberseguridad. Estos descubrimientos evidenciaron la carencia de certificaciones y revisiones obligatorias en materia ciberseguridad en productos sanitarios, comercializados actualmente. Desgraciadamente la falta de

presupuesto dedicado a investigación no permitió la adquisición de varios dispositivos médicos, para su posterior evaluación en ciberseguridad.

Conclusiones

La realización de los trabajos e investigaciones previamente mencionadas permitió obtener las siguientes conclusiones. Partiendo de la necesidad en mecanismos de ciberseguridad de las infraestructuras sanitarias, se debe tener en cuenta su particularidad diseño y funcionamiento. Las pruebas y mecanismos de ciberseguridad diseñados han de ser aplicables en entornos reales. Desgraciadamente actualmente en las infraestructuras sanitarias hay sistemas tecnológicos imposibles de actualizar o modificar. Multitud de máquinas de tratamiento y diagnostico cuentan con software y sistemas operativos propietarios a los cuales los administradores y empleados no tienen acceso. Teniendo en cuenta esta situación, se deben desarrollar medidas que permitan su aplicación en este ecosistema y que en la medida de los posible puedan reducir y paliar el riesgo ofrecido por estos sistemas.

Esta conclusión viene ligada a la falta de seguridad en dispositivos médicos. La mayoría de los dispositivos médicos no han seguido un proceso de diseño seguro y no han sido sometidos a pruebas de seguridad por parte de los fabricantes, al suponer esto un coste directo en el desarrollo del producto. La única solución en este aspecto es la aplicación de una legislación que fuerce a los fabricantes a cumplir estándares de seguridad. Y aunque actualmente se ha avanzado en este aspecto regulatorio, se tardaran años o décadas en sustituir los dispositivos inseguros. La imposibilidad de actualizar, o fallos relacionados con el hardware de los productos, hacen imposible la solución de todos los fallos de seguridad que se descubran. Abocando al reemplazo del dispositivo, cuando exista una alternativa satisfactoria en materia de ciberseguridad. Por esta razón es necesario diseñar nuevos mecanismos de ciberseguridad que puedan ser aplicados actualmente y puedan mitigar estos riesgos en este periodo de transición.

Finalmente, en materia de robo de datos. Aunque las investigaciones preliminares realizadas en esta tesis no consiguieron realizar ningún descubrimiento significativo en el robo y venta de datos. Actualmente las darknets, en concreto la red Tor [15], se han convertido un punto clave en el modelo de Ransomware as a Business (RaaB) [5], al ofrecer sitios webs de extorsión y contacto con estos grupos.

Abstract

The development of novel cybersecurity detection methods has failed to stop the increase in cybersecurity incidents. This has led to a difficult situation, where many companies are being affected by cybersecurity incidents [2][3][4][5]. The development of measures capable of stopping and detecting these attacks is especially relevant in critical infrastructures, such as healthcare services. In this thesis, a cybersecurity review, analysis of threats and development of novel cybersecurity techniques is presented. This thesis follows an experimental and deductive method consisting of three papers. The first paper is centred on developing new techniques of malware detection based on the usage of artificial intelligence. This research was able to develop a method for detecting potentially unwanted and malicious applications in mobile environments. The second publication looked to identify and detect threats and stolen information from healthcare services on darknets [13]. This research led to the discovery and proof of the interconnection between different darknets. The last publication is focused on analyzing the security of medical devices. To carry out this research, a medical device, a portable electrocardiograph [14], was tested. These tests were able to discover multiple cybersecurity vulnerabilities. Proving the necessity for the development of novel detection and protection methods applicable to the Healthcare Industry. On top of that, multiple medical devices present minimal or no cybersecurity features. It is necessary to develop transition contingency measures. The usage of medical devices with cybersecurity features by healthcare services will probably be a process that will not be achieved in years but decades. Finally, regarding stolen information, darknets; in particular the Tor network [15], have become a key point in the Ransomware as a Business (RaaB) model [5]. Several of the victims publicised by these groups have turned out to be health services [16][17], proving the need and interest in the study of such networks.

"We can only see a short distance ahead, but we can see plenty there that needs to be done."
Alan Turing

Table of Contents

List of Tables

Chapter 1

Introduction

1.1 Introduction

Cybersecurity, or computer security, is not a novel concept of our day. Since the beginning of communications and connection development between computers, in the early 1960s, cybersecurity has been a topic of discussion. One of the first conference panels focused on this topic was held by RAND researcher Willis H. Ware [18] at the Spring Joint Computer conference in Atlantic City in 1967, where several cybersecurity papers were presented [1]. One of the presented papers was 'Security considerations in a multi-programmed computer system' by Bernard Peters a member of the United States National Security Agency (NSA) [19]. This paper is a piece of special interest due to some of its statements, that are still applicable today.

Bernard Peters starts his paper with the following statements:
'Security can not be attained in the absolute sense. Every security system seeks to attain a probability of loss which is commensurate with the value returned by the operation being secured. For each activity which exposes private, valuable, or classified information to possible loss, it is necessary that reasonable steps be taken to reduce the probability of loss. Further, any loss which might occur must be detected.'[19].

Those statements are still perfectly valid and applicable in 2022. Through the years those statements have been proved and evolved into new terms, definitions and methodologies, being one of them Zero Trust Security Mode, also known as Zero Trust Architecture (ZTA). The main concept behind the "zero trust" concept is "never trust, always verify", and follows the previously mentioned idea that security can not be attained in the absolute sense. This term was coined in 1994 by Stephen Paul Marsh in his doctoral thesis[20]. Later on, in 2018, cybersecurity researchers at NIST[1] and the NCCoE[2] published the SP 800-207, Zero Trust Architecture (ZTA)[21]. This publication contains and defines a cybersecurity architecture base on the Zero Trust(ZT) principle. These recent design architectures, once again, follow and try to solve the statements made by Bernard Peters in 1967, *'For each activity which exposes private, valuable, or classified information to possible loss, it is necessary that reasonable steps be taken to reduce the probability of loss.'*. ZTA offers plans and methodologies, based on zero trust concepts, to improve the cybersecurity of organizations.

Even though most of the principles stated by Bernard Peters are still valid, cybersecurity has evolved through the last decades. ZTA is the result of a process of evolution, being one of the most modern security architectures, but previously to ZTA numerous attempts have been done and replaced. ZTA moves the main defensive paradigms from static, network-based perimeters to users, assets, and resources. For instance, earlier security models were heavily focused on network-based architectures[22][23] that were proved insufficient with

[1] https://www.nist.gov/

[2] National Cybersecurity Center of Excellence

the emergence of mobile devices like smartphones o computer laptops. It is necessary to mention that some of those techniques are still considered good cybersecurity practices, like network segmentation[24], but they need to be supported by other cybersecurity policies and actions.

Nowadays current novel methods of detection are based on continuous monitoring of all technological systems[25][26]. Based on the fact that any system can be affected by a cyberattack, even if they are not connected to the internet[27], it is necessary to monitor all possible systems for early detection and response against any possible cyberattack. Following this path of monitoring and data collection most of the recent studies and industry development products has been using machine learning and deep learning methods to detect cyberattacks[28][29] (e.g., anomaly detection systems[30], malware detection[31][32], spam detection[33] and digital forensics[34]).

Modern cybersecurity has acknowledged the fact, that a cybersecurity incident is inevitable at some point. Measures need to be done to delay successfully incidents and assure a fast and efficient incident response. In modern times, the cybersecurity maturity of an organization is usually measured and tested when they are handling cybersecurity incidents. Well-prepared organizations, in most cases, will successfully manage cybersecurity incidents without affecting critical systems. Where organizations without enough cybersecurity measures, at an organizational and technical level, tend to fall into chaos, and in most cases pay enormous amounts of money to ransomware gangs [35][36].

1.1.1 Definition of the problem

Unfortunately, the development of novel cybersecurity detection methods has failed to stop the increase of cybersecurity incidents. Methods of attack, evasion techniques and attackers has also evolved throw the years. Being, right now, one the most popular incidents the one knows as ransomware attacks [2][3]. A report released by the US Treasury's Financial Crimes Enforcement Network (FinCEN) detected a massive growth in ransomware payments in 2021 [4].

Furthermore, most recently digitalised sectors have proven to be less mature in terms of cybersecurity. Multiple Industrial Control Systems(ICS) were kept isolated from the Internet, but now, are being increasingly connected without the necessary cybersecurity recommendations [37]. Besides, the industrial sector and ICS have their own peculiarities and necessities, that turn them into a specific cybersecurity problem. Being necessary, the development and design of specific cybersecurity protection methods for the industry sector.

Among the newly digitalised sectors is the healthcare industry. Healthcare services are constantly adding technological solutions, since novel diagnosis systems [38][39], to the use of robotics[40] or new ways of communication between medical personal and patients [41]. This phenomenon is commonly called 'digital health' [12]. Furthermore, Healthcare Industry is one of the largest and most important industries in the world. According to Statista just in the United States Health Care & Social Assistance obtained a revenue of $2,612 billion in 2020 [42]. Moreover, the digital health market was valued at $ 66.5 billion in 2021 and is expected to grow at a compound annual growth rate (CAGR) of 26.9% from 2022 to 2030, according to a report by Grand View Research, Inc [43]. For these reasons, and being an expanding digitalized sector, without a previous focus on cyber security, the health sector has been affected by multiple cyberattacks [7][11][8][9].

These attacks proved the need for novel cybersecurity protection systems. And similar to other Industry Sectors, Healthcare Industry needs specific designs and tailored solutions as many of its systems are critical and affect human lives. For example, all possible cybersecurity development systems that need to deal with medical equipment must comply with safety measures to not alter their normal functionality. Cybersecurity proposals and ideas need to adjust to these scenarios to be actually applicable. A software failure in medical systems could end up costing human lives.

Therefore the work of this thesis has been focused on how to improve and detect cybersecurity problems in the Healthcare Industry. But with a focus on the applicability and study of the research.

1.2 Research objectives

The objectives of this thesis are listed below:

1. Objective 1. The study of the usage and development of machine learning techniques to enhance the cybersecurity protection applicable to mobile devices
2. Objective 2. To analyse the structure of darknets in order to understand criminal activities and threats related to the Healthcare Industry
3. Objective 3. The study of the cybersecurity status of modern IoT medical devices

1.3 Literature Review

In this section, a literature review will be presented, addressing the current research about cybersecurity in general critical infrastructures, such as healthcare services. Since the healthcare industry is categorized as critical infrastructure, a detailed literature review of research performed in different critical infrastructure scenarios will also be included. In addition, special attention will be given to empirical research because of its most valuable scientific contribution.

1.3.1 Critical Infrastructures and Healthcare cybersecurity

Critical Infrastructure Cybersecurity is different to traditional company cybersecurity, due to the sensitive nature of these infrastructures and their peculiarities, such as specific industrial protocols (e.g, Modbus) and their repercussions in the event of failure. Furthermore, it is necessary to understand that most of these critical infrastructures were designed without an internet connection in mind, and their security has been provided by isolation. In a world where everything is being connected to the Internet, protecting those infrastructures is a challenge. Back in 2013, the White House published an executive order [44] commanding the improvement of critical infrastructure cybersecurity.

Following this command the National Institute of Standards and Technology has been working on developing a Framework for Improving Critical Infrastructure Cybersecurity[45], being its last version the one from 2018[46]. This framework is an ongoing collaborative effort that involves industry, academia and government, to improve cybersecurity risk management in critical infrastructures. Several academic research works have been focused on reviewing the recent threats and attacks[47][48]. The research studies made by CS Kruse *et al.*[49] and Lynne Coventry *et al.*[50] specifically performed a review of modern threats and trends in healthcare cybersecurity. Regarding possible solutions proposals, researchers such as AJ Coronado *et al.* have proposed security improvement solutions based on risk management[51]. Other researchers have been focused on evaluating and detecting cybersecurity failures in medical devices. Jake L Beavers *et al.* successfully identified multiple cybersecurity vulnerabilities in pacemakers and Eduard Marin *et al.* identified vulnerabilities in Implantable Cardiac Defibrillators(ICDs)[52]. Moreover, non academia researchers has also identified multiple cybersecurity vulnerabilities in medical devices[53][54][55]. These discoveries also led to the design of proposal of several mechanisms of protection for medical devices, acting like proxies to protect against eavesdropping or malicious communications[56][57].

On the other hand, there is also numerous research centred on SCADA (Supervisory Control and Data Acquisition) systems. Since the design of vulnerability assessments systems[58], risk assessment methods[59] or cybersecurity considerations[60]. Unfortunately, even though SCADA systems are related to critical infrastructure management, they are usually installed or operated in healthcare centres. Healthcare centres have their own particular issues that need to be addressed and studied in detail.

Finally, other contributions are centred on the need for effective regulations that force the implementation of cybersecurity measures[61][62]. A Strielkina *et al.* performed a regulation and case-oriented assessment about the cybersecurity of IoT-based systems used in healthcare[63]. Regulations will force organisations to comply with security measures, improving the detection of handling of cyber incidents. But will also force medical device manufactures to comply with cybersecurity standards.

Possible solutions to cybersecurity in healthcare services still raise multiple problems and research questions, being this situation is one of the motivating aspects of this thesis. It is necessary to research and develop new methods of cybersecurity for healthcare institutions. Being aware of this situation and following these premises, the European Commission has acknowledged these problems and has dedicated specific research funding to Healthcare Security[64][65][66]. In Horizon 2020 (H2020), one of the largest European funding program for research and innovation, the European Union funded with 35 million Euros several Research and Innovation actions [64][65]. And in Horizon Europe, the new European research and innovation funding program, there is a specific research topic dedicated to Enhancing the cybersecurity of connected medical devices[66]. One example of this research and innovation actions was ProTego [67]. The University of Alcalá was part of the ProTego project, under some part of the research carried out in this thesis has been conducted.

1.4 Contributions

Any detailed analysis of the state of the art related to cybersecurity in healthcare will discover multiple works presenting cybersecurity challenges [68] and the modelling of modern threats based on risk analysis [69][70]. But, at the moment of writing this thesis, there is a lack of applied research in this field. As mentioned before, the European Commission also has acknowledged the necessity of applying and researching novel cybersecurity methods for Healthcare Services. Several of those Research and Innovation actions were focused on developing Trusted digital solutions and Cybersecurity in Health and Care, being this a specific challenge in H2020. As a consequence of this situation, the work of this thesis has been extremely focused on applied research, and several experiments and evaluations have been performed. These works gave as result several publications indexed in the Journal Citation Report (JCR) index, which are detailed and presented in the following sections.

Impact of Article 1

Title	C. Cilleruelo, Enrique-Larriba, L. De-Marcos and J.J. Martinez-Herráiz, "Malware Detection Inside App Stores Based on Lifespan Measurements," in IEEE Access, vol. 9, pp. 119967-119976, 2021, doi: 10.1109/ACCESS.2021.3107903.
Summary	Potentially Harmful Apps (PHAs), like any other type of malware, are a problem. Even though Google tries to maintain a clean app ecosystem, Google Play Store is still one of the main vectors for spreading PHAs. In this paper, we propose a solution based on machine learning algorithms to detect PHAs inside application markets. Being the application markets one of the main entry vectors, a solution capable of detecting PHAs submitted or in submission to those markets is needed. This solution is capable of detecting PHAs inside an application market and can be used as a filtering method, to automatically block the publishing of novel PHAs. The proposed solution is based on application static analysis, and even though several static analysis solutions have been developed, the innovation of this system is based on its training and the creation of its dataset. We have created a new dataset that uses as criteria the lifespan of an application inside Google Play, the shorter time an application is active inside an application market the higher the probability that this is a PHA. This criterion was added in order to avoid the usage and bias of antivirus engines for detecting malware. Involving the lifespan as criteria we created a new method of detection that does not replicate any existing antivirus engines. Experimental results have proved that this solution obtains a 90% accuracy score, using a dataset of 91,203 applications published on the Google Play Store. Despite showing a decrease in accuracy, compared with other machine learning models focused on detecting PHAs; it is necessary to take into account that this is a complementary and different method. The presented work can be combined with other static and dynamic machine learning models, since its training is drastically different, as it was based on lifespan measurements.
Impact	This paper has been published in IEEE Access. IEEE Access is a peer-reviewed open-access scientific journal published by the Institute of Electrical and Electronics Engineers (IEEE). In the Science Index of Journal Citation Reports 2021, its Impact factor is 3.476. And is ranked 79th of 164 (Q2) in the category COMPUTER SCIENCE, INFORMATION SYSTEMS, the rank 43rd of 94 (Q2) in the category TELECOMMUNICATIONS and the rank 105 of 276 (Q2) in the category ENGINEERING, ELECTRICAL & ELECTRONIC. Under Journal Citation Indicator (JCI) 2021 its score is 0.93. Holding the rank 75th of 246 (Q2) under the category COMPUTER SCIENCE, INFORMATION SYSTEMS, the rank 44th of 116 (Q2) under the category TELECOMMUNICATIONS and the rank 104th of 344 (Q2) under the category ENGINEERING, ELECTRICAL & ELECTRONIC. Finally under the Scopus CiteScore Rank 2021 its CiteScore: 6.7, SJR: 0.927 and SNIP: 1.326. And is ranked 28th of 300 (90th percentile) in the category Engineering, General Engineering, the rank 34th of 231 (85th percentile) in the category Computer Science, General Computer Science and the rank 104th de 455 (77th percentile) in the category Materials Science, General Materials Science.

Table 1.1: Impact paper 1

Impact of Article 2

Title	C. Cilleruelo, L. de-Marcos, J. Junquera-Sánchez and J.J. Martínez-Herráiz, "Interconnection Between Darknets," in IEEE Internet Computing, vol. 25, no. 3, pp. 61-70, 1 May-June 2021, doi: 10.1109/MIC.2020.3037723.
Summary	Tor and i2p networks are two of the most popular darknets. Both darknets have become an area of illegal activities highlighting the necessity to study and analyze them to identify and report illegal content to law enforcement agencies (LEAs). This article analyzes the connections between the Tor network and the i2p network. We created the first dataset that combines information from Tor and i2p networks. The dataset contains more than 49k darknet services. The process of building and analyzing the dataset shows that it is not possible to explore one of the networks without considering the other. Both networks work as an ecosystem and there are clear paths between them. Using graph analysis, we also identified the most relevant domains, the prominent types of services in each network, and their relations. Findings are relevant to LEAs and researchers aiming to crawl and investigate i2p and Tor networks.
Impact	This paper has been published in IEEE Internet Computing. IEEE Internet Computing is a bimonthly peer-reviewed scientific journal published by the IEEE Computer Society. In the Science Index of Journal Citation Reports 2021, its Impact factor is 2.680. Holding the rank 43rd of 110 (Q2) in the category Computer Science, Software Engineering. Under the Journal Citation Indicator (JCI) 2021 its score is 0.92. And holds the rank 37th of 133 (Q1) in the category Computer Science, Software Engineering. Finally under the Scopus CiteScore Rank 2021, its CiteScore is 6.2, SJR: 1.03 and SNIP: 1.389. And holds the rank 77th of 359 (77th percentile) in the category Computer Science, Computer Science Applications.

Table 1.2: Impact paper 2

Impact of Article 3

Title	C. Cilleruelo, J. Junquera-Sánchez, L. de-Marcos, N. Logghe and J.J. Martinez-Herraiz, "Security and privacy issues of data-over-sound technologies used in IoT healthcare devices," 2021 IEEE Globecom Workshops (GC Wkshps), 2021, pp. 1-6, doi: 10.1109/GCWkshps52748.2021.9682007.
Summary	Internet of things (IoT) healthcare devices, like other IoT devices, typically use proprietary protocol communications. Usually, these proprietary protocols are not audited and may present security flaws. Further, new proprietary protocols are desgined in the field of IoT devices, like data-over-sound communications. Data-over-sound is a new method of communication based on audio with increasing popularity due to its low hardware requirements. Only a speaker and a microphone are needed instead of the specific antennas required by Bluetooth or Wi-Fi protocols. In this paper, we analyze, audit and reverse engineer a modern IoT healthcare device used for performing electrocardiograms (ECG). The audited device is currently used in multiple hospitals and allows remote health monitoring of a patient with heart disease. For this auditing, we follow a black-box reverse-engineering approach and used STRIDE threat analysis methodology to assess all possible attacks. Following this methodology, we successfully reverse the proprietary data-over-sound protocol used by the IoT healthcare device and subsequently identified several vulnerabilities associated with the device. These vulnerabilities were analyzed through several experiments to classify and test them. We were able to successfully manipulate ECG results and fake heart illnesses. Furthermore, all attacks identified do not need any patient interaction, being this a transparent process which is difficult to detect. Finally, we suggest several short-term solutions, centred in the device isolation, as well as long-term solutions, centred in involved encryption capabilities.
Impact	This paper has been published in the IEEE Global Communications Conference (GLOBECOM) 2021. The Global Communications Conference is an annual international academic conference organised by the IEEE. This conference is included under the GII-GRIN-SCIE (GGS) Conference Rating 2021 (update October 24, 2021), having a scoring of GGS Class 2. Furthermore this conference is included in the index Computer Research and Education (CORE) 2020, under Rank. "B"

Table 1.3: Impact paper 3

1.4.1 Summary of the contribution

This thesis, as shown by the previously mentioned papers, contributes to providing answers on how to detect and improve cybersecurity in a critical industry such as Healthcare.

The three previous scientific publications seek to provide answers about the cybersecurity status of the industry and test novel security methods. Each one of the papers is focused on different techniques and answers specific research objectives but all of them share a common background in healthcare services. Each one of the papers has been focused in solve each one of the objectives presented in this thesis.

- Objective 1. The study of the usage and development of machine learning techniques to enhance the cybersecurity protection applicable to mobile devices has been addressed in the first paper, Malware Detection Inside App Stores Based on Lifespan Measurements
- Objective 2. To analyse the structure of darknets in order to understand criminal activities and threats related to the Healthcare Industry, has been addressed in the second paper, Interconnection Between Darknets
- Objective 3. The study of the cybersecurity status of modern IoT medical devices, has been addressed in the third and final paper of this thesis, Security and privacy issues of data-over-sound technologies used in IoT healthcare devices.

1.5 Thesis structure

The thesis follows is structured in the following way. In this introduction chapter a state of the art, a summary of the impact of scientific publications and the relationships between them is presented. Following this chapter, the three papers are then presented, followed by a discussion of the results, conclusions and lines of future work.

- Chapter 2 presents the first paper of the thesis, concerning the research and use of machine learning algorithms applied to cybersecurity. This paper is the starting point of the research and studies on how to apply cybersecurity techniques to a specific environment, such as Healthcare.
- Chapter 3 presents the second paper of the thesis, which analyzed and proves the connection between different darknets. This discovered was made during a research process that tried to identify threats against this critical industry and raise some questions about how malicious actors operate.
- Chapter 4 presents the third paper of the thesis, where the security of an electronic health device is evaluated. This novel IoT device in charge of taking electrocardiograms is subject to a cybersecurity audit process. Achieving the discovery and identification of several vulnerabilities.
- Chapter 5 presents a discussion of the combined results of the three papers. And finally, chapter 6 offers a summary of the different conclusions and possible future lines of work.
- In relation to the bibliography, each one of the presented papers includes a section where its references are shown. In addition to this, the references used in the remaining sections are listed at the end of this thesis.

Chapter 2

Mobile malware detection using machine learning techniques

2.1 Paper 1 contribution

Like in any other industry smartphones are actively used in hospitals and other healthcare centres. Mobile phones are not only a way of communication, they have turned into a method of scheduling medical appointments, checking for medical results or even medical consultation, through remote video conferences or calls. This concept is known as telehealth or telemedicine [71] and it can be defined as the distribution of health-related services and information via electronic information and telecommunication technologies. Furthermore, due to the recent Covid19 [72], these medical care methods have been extensively used. In some cases, remote communication or medical follow-up has become the only possible way of communication. These situations have led to the need to provide smartphones to all medical personnel. And, usually, as in most industries and companies, healthcare centres had applied a Bring Your Own Device (BYOD) policy. BYOD is a company policy that allows employees to bring and use their own devices, during their workday. This policy avoids company purchases of mobile phones for employees, offering cost savings to the company. But create other security problems and concerns.

First of all, in a BYOD environment personal and medical, or work-related, information is not isolated. Medical personal share the same device for private affairs and patient data or results. Also those devices, nowadays, represent a fundamental part of the work of medical personnel. Not only results or patient data: medical appointments, access to the hospital emails, work schedules and other necessary information for the proper functioning of the hospital can be stored there.

Due to those facts, it is necessary to study new ways of improving mobile device protection. And also research possible ways of adding security to multiple,and from different vendors, mobile devices. One problem of BYOD, apart from the non-separation of personal and work-related data, is the variety of devices. The variety of devices makes it difficult to create easily deployable solutions that can cover multiple vendors and device types. Novel solutions should be aware of that, and try to be easily applicable to multiple mobile devices of different vendors.

One possible solution to these aspects is to protect and improve the detection of Potentially Harmful Apps (PHAs). Most mobile applications are installed through official app stores, such as Google Play Store [73]. PHAs developers are aware of that and published malicious software in app stores [74]. So one way of improving the security of the mobile ecosystem, in a generic way that can affect multiple vendors, is to improve the detection and block of PHAs in app stores. In this chapter, a new method of detection inside App Stores that used machine learning algorithms is presented. Detection and reducing PHAs inside app stores will directly affect the security of multiple mobile devices, including the devices of medical personnel. This does not mean that all PHAs will disappear but greater control over app stores will force malware developers to use and study alternative techniques.

2.2 Paper 1

The first scientific paper is included below, “Malware Detection Inside App Stores Based on Lifespan Measurements”.

Received July 26, 2021, accepted August 11, 2021, date of publication August 25, 2021, date of current version September 7, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3107903

Malware Detection Inside App Stores Based on Lifespan Measurements

CARLOS CILLERUELO, ENRIQUE-LARRIBA, LUIS DE-MARCOS, AND JOSE-JAVIER MARTINEZ-HERRÁIZ

Computer Science Department, University of Alcalá, 28801 Alcalá de Henares, Spain

Corresponding author: Carlos Cilleruelo (carlos.cilleruelo@uah.es)

This work was supported by the European Union's Horizon 2020 Research and Innovation Program under Grant 826284 (ProTego).

ABSTRACT Potentially Harmful Apps (PHAs), like any other type of malware, are a problem. Even though Google tries to maintain a clean app ecosystem, Google Play Store is still one of the main vectors for spreading PHAs. In this paper, we propose a solution based on machine learning algorithms to detect PHAs inside application markets. Being the application markets one of the main entry vectors, a solution capable of detecting PHAs submitted or in submission to those markets is needed. This solution is capable of detecting PHAs inside an application market and can be used as a filtering method, to automatically block the publishing of novel PHAs. The proposed solution is based on application static analysis, and even though several static analysis solutions have been developed, the innovation of this system is based on its training and the creation of its dataset. We have created a new dataset that uses as criteria the lifespan of an application inside Google Play, the shorter time an application is active inside an application market the higher the probability that this is a PHA. This criterion was added in order to avoid the usage and bias of antivirus engines for detecting malware. Involving the lifespan as criteria we created a new method of detection that does not replicate any existing antivirus engines. Experimental results have proved that this solution obtains a 90% accuracy score, using a dataset of 91,203 applications published on the Google Play Store. Despite showing a decrease in accuracy, compared with other machine learning models focused on detecting PHAs; it is necessary to take into account that this is a complementary and different method. The presented work can be combined with other static and dynamic machine learning models, since its training is drastically different, as it was based on lifespan measurements.

INDEX TERMS Machine learning, app stores, google play malware, android malware, malware detection, potentially harmful apps.

I. INTRODUCTION

Malware detection techniques are constantly evolving due to the necessity of detecting the presence of malware. Cybercriminals are constantly changing their techniques and novel methods of detection are needed to be developed. Moreover, Android has become one of the most popular operating systems in mobile devices. According to Statcounter, Android has a market share greater than 72% [1]. This situation has caused an increase in the malware ecosystem because of its popularity [2], [3]. All of this is related to the rise of smartphone users worldwide, more than 6 billion in 2021 [4]. Due to this situation, cybercriminals are increasing attacks against smartphones and the Android ecosystem in particular. On top of that, we should take into account that even in the latest Android version 11, the system still allows installing applications from unverified sources. Several malware SMS campaigns, using SMiShing techniques [5], had exploited this possibility [6], [7] but the use of markets, third-party markets, and the official Google Play Store, is still the main distribution vector of infection for most Android malware [8]. Being Google Play Store the main distribution vector, novel techniques that control who published and which applications are published need to be developed. This evaluation is currently a challenge since there are around nearly 3 million applications in Google Play Store [9], making it difficult to evaluate all of them. A proposed solution should be applicable to all published applications and also have an acceptable evaluation and detection time. In 2017 Google tried to accomplish a solution to this problem by developing a system

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

called Google Play Protect [10]. Google Play Protect is a security measure that has managed to block, just in 2017, approximately 10 million harmful app installations [11]. However several studies [12], and the current situation of Android malware inside the Google Play Store [8], [13], has proved this technology inefficient. The incapacity or disregard from Google has been evidenced due to the number of malware campaigns in Google Play Store [14], [15]. And it is necessary to take into account that Android allows several alternative markets where there are even more malware applications [16]. Better detection rates are needed to fight malware inside application markets.

Furthermore, we should not forget the emergence of the Internet of Things (IoT) ecosystem and the use of Android as its operating system in these environments [17], [18]. These ecosystem also needs novel methods of malware detection [19], [20]. Those Android IoT devices can also incorporate the usage of application markets, for this a solution that grants better control over application markets will benefit, not only smartphones but also the full Android ecosystem.

Within this context, it is important to research and apply new methods of PHAs detection. Moreover, these new detection methods need to be applicable in the real world and take into account applications particularities. For example, there are devices, like Samsung, with a proprietary software development kit(SDK) that can use specific permissions like, samsung.accessory.permission.ACCESSORY_FRAME WORK. These permissions can only be found in certain devices and have been normalized or removed to guarantee a multi-platform market solution. It is not real to create novel detection methods that do not take into account these peculiarities or are based on unique features like C&C domains or IP addresses.

In this paper, we present a novel method of detection based on lifespan measurements that can be used for detecting malware in application markets. This is a lightweight method that makes it possible to easily scan millions of applications in a feasible time. For example, newer applications submissions can be processed through this detection method, without significantly affecting the publication process. We developed an automatic solution based on static analysis techniques but taking into account the previous mentioned particularities of the Android application ecosystem. The features used by this system have been carefully normalized and can be present in any Android application. These features are divided into groups like Permissions, Hardware, or Google Play Store categories. This approach also generates a lightweight design, that contributes to its easier implementation. Only 601 application features are used in the training and evaluation methods. But the main difference with other detection methods is the PHAs dataset composition and its use in the creation of this detection system.

A dataset of 91,203 applications, published inside the Google Play Store has been utilized for this research. To split the applications into legitimate or PHAs a new classification criterion has been applied. Instead of just using know antivirus engines to classify the samples, the lifespan of mobile applications inside the Google Play Store has also been used as a selection criterion.

In summary, a list of contributions of this paper are the following:

- *Unique dataset*. We systematically created and labelled a dataset based on applications lifespan inside the Google Play Store. This dataset is publicly accessible in GitLab, https://gitlab.com/ciberseg-uah/public/pha-android-dataset
- *New method of detection of PHAs*. Using the previously mentioned dataset, we created a new method of PHAs detection. This method is based on machine learning techniques and involves this lifespan measure as a selection criteria.
- *Antivirus Engines Bias Avoidance*. The use of our classified dataset avoids the bias produced by antivirus engines. We are not replicating the behaviour of an antivirus engine, but creating a new detection method.
- *Explainable Results*. The proposed method has been tested and trained using different machine learning models and techniques. These techniques are explained and analyzed in this research paper. All machine leanings algorithms in this research allow obtaining explainable results.
- *Lightweight training and Feature Selection*. In order to create a heterogeneous solution for the Android ecosystem, we reduce and normalized the application features to common ones. The system only uses 601 features for the training and evaluation of applications instead of thousands of features. Also, being a static analysis detection method, the model presents a Mean time to detect (MTTD) smaller than one second per application.

All these contributions follow practical use. This system, created using machine learning techniques, could be used for the early detection of malicious campaigns inside application markets. And for early detection of PHA before its publication inside the market. Multiple PHAs could be detected during the submission and validation process made by application markets.

II. BACKGROUND AND RELATED WORK

Day to day, malware evolves to pretend it is a legitimate program, increasing the complexity of the detection process. Furthermore, malware detection leads to another problem. There are cases where there is not a clear line to distinguish malware. Different antivirus engines have different criteria when classifying samples [21] Hurier *et al.* clearly state this lack of consensus in antivirus engines [22]. Antivirus used a threshold in order to consider a malware sample. Hurier *et al.* also stated that there is no public theory or golden rule behind the selection of this threshold. Finally, their work concludes by explaining the necessity of novel detection methods and the use of aggregated antivirus decisions for avoiding bias. Harmful applications may be detected by some antivirus and in other cases being classified as benign or detected as malware but classified in different categories of malware. Each antivirus engine has different policies dealing with PHAs, occasionally more relaxed or restrictive, on malware analysis [23]. For example, some of them could have heavy policies against adware, and others tolerate this type of PHAs.

Malware analysis may involve different methodologies and techniques. Some of them base their classification on the recognition of known patterns on the program code [24]. If a certain code has been previously detected on security incidents, it will be remembered and detected by the antivirus engines, regardless of the machine in which it is executed. This analysis is usually done through static analysis, an analysis performed without actually executing programs.

Another technique used in malware analysis is dynamic analysis. When classifying new malware samples which have never been detected before, remembering patterns on the code does not improve the identification [24]. It is necessary to execute an analysis of the application while it is being executed to verify that its functionalities are the ones expected. Dynamic analysis has been used in malware detection [25], [26] and has been proven effective thanks to the information provided, which describes a program and its behaviour.

The classification of samples is a problem that requires the recognition of patterns on a data set. Static and dynamic malware analysis can provide a lot of features and patterns of PHAs. Due to its ability to recognize patterns, Machine Learning is a good technology for the implementation of novel detection methods. It offers several algorithms capable of find patterns and classify data based on certain features. Even so, it is needed to supervise the training by specifying the class to which samples belong.

The use of Machine Learning, for classifying mobile applications, has been involved in a multitude of studies [27], [28] [29]. Some researchers had used Support Vector Machines (i.e. SVM) [30]. Others have used algorithms like Random Forest Classifier (i.e. RFC) and Linear Regression [31] to classify applications.

There have been several studies applying machine learning to detect PHAs [30], [32] [33]. One of the most relevant studies is Drebin [30]. Drebin achieves a detection rate of 94% using 545,000 different features. But from our point of view, several features should not be considered (e.g., Network addresses, application-defined permissions, activities' names). Malware is easily mutable and training a machine learning model with unique characteristics will not improve the detection rate. It is necessary to generate a dataset with common characteristics that all the PHAs could have.

Another research related to Android malware classification that uses a more generic approach selecting features of a dataset [34] is APK Auditor. APK Auditor [34] uses Android permissions, common features between applications to create a permission-based model obtaining a detection rate of 88%. Even though the accuracy of APK Auditor is lesser than Drebin, APK Auditor is a better approach to malware detection. In a real-world environment, the accuracy of APK Auditor will be better than Drebin due to the evaluation of common features between samples. On the other hand, other recent studies have also proved the effectiveness of machine learning in dealing with Android IoT malware. [35], [36]

III. METHODOLOGY

A. AVOIDING ANTIVIRUS DETECTION BIAS

First of all, we created a novel dataset using Tacyt.[1] Tacyt is a cyber-intelligence tool developed by ElevenPaths, a cybersecurity company subsidiary of Telefónica Digital España, S.L. This tool performs a crawling of different mobile application markets, including the Google Play Store. This process downloads and then performs a static analysis of millions of mobile applications. Using this tool we were able to access a database of 273,662 applications, published inside the Google Play Store between 22th of January 2010, and 11th of July 2018. Those applications allowed us to create a labeled dataset of 91,203 applications. Tacyt provides information about each application, like the Android Package (APK) files and dates associated with the Google Play Store publication or its publishing category. This allows its subsequent analysis, even after the application has been deleted from the market.

There are several public PHAs datasets [37], [38] already accessible but to present an innovative way of detection we did not use any of them. Those datasets use antivirus engines as a classification method. Also none of the recently published datasets involve application store lifespan measurements to their building. AndroCT [39] and TraceDroid [40] present static and dynamic analysis data but do not give any metric related to lifespan. Moreover, recent works combined static and dynamic analysis, like Cai *et al.* [41], Cai and Ryder [42] which studied application structure and behaviours and then create an application classification approach base on that information. Cai *et al.* [43] also studied the evolution of benign and malign applications in the Android ecosystem to understand its behaviours. But again the previously mentioned approaches did not specifically study applications published in application markets and did not involve lifespan measurements. It is necessary to understand that the novelty of this work is not based on the application of static analysis, a technique widely tested and studied in numerous research papers [30], [44] [45].The novelty of the proposed machine learning model is based on its new method of dataset creation. First of all, the dataset creation takes into account the antivirus bias problem and involve a new selection method based on lifespan measures. As this method is specifically designed to be used in application stores, lifespan measures are taking based on the lifespan of applications inside those stores. Additionally to these unique characteristics, this method can be combined with previous methods, due to its different creation and behaviour. This novel method can be combined with previous ones as an ensemble learning method, improving previous detection rates.

[1] https://www.elevenpaths.com/es/tecnologia/tacyt/index.html

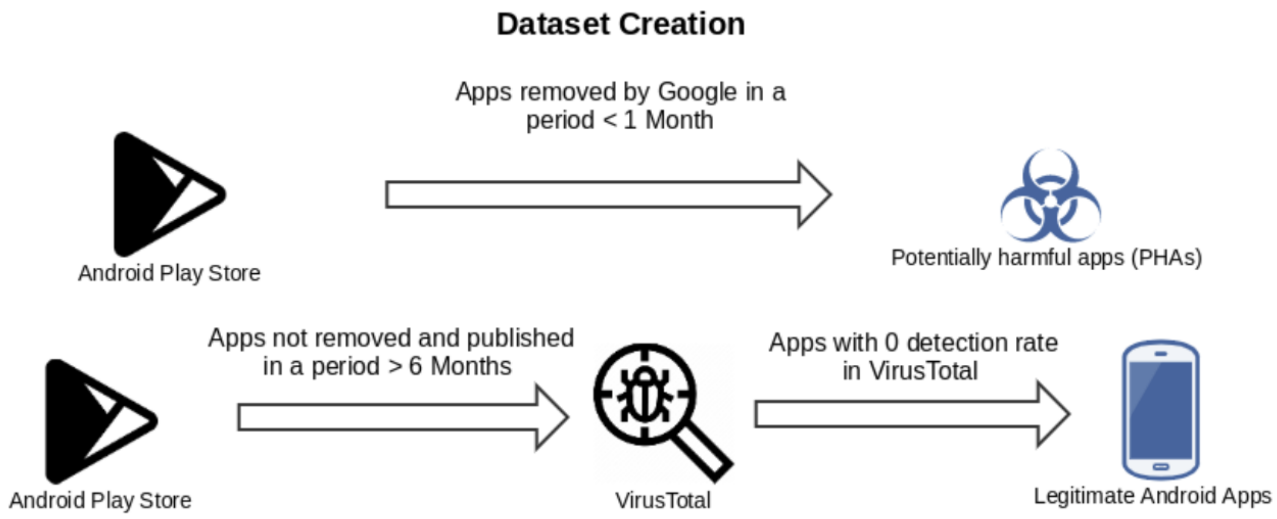
Dataset Creation
Apps removed by Google in a period < 1 Month
Android Play Store
Potentially harmful apps (PHAs)
Apps not removed and published in a period > 6 Months
Apps with 0 detection rate in VirusTotal
Android Play Store
VirusTotal
Legitimate Android Apps

FIGURE 1. Method used in order to select applications for the dataset.

In our use case, since we are using supervised learning algorithms, we also need to define which applications can be considered PHAs and which ones are not. As previously mentioned, distinguish between PHAs and legitimate applications is a problem. In multiple cases, there is not a clear line that differentiates between benign and malicious apps. This also happens using antivirus decision engines, several antivirus engines can provide different results analyzing the same application. Moreover, if we classify our samples based on antivirus decision engines we will be only replicating their judgment and not creating a new one.

The proposed approach is based on considering as PHAs android applications that have been banned from the Google Play Store market. Those applications could be considered harmful to the user, so they should be detected by the machine learning model. At the moment of writing this article, Google does not publicly share any information of banned applications from the Google Play Store. The strategy followed by this research uses Tacyt to access the publishing and removal dates of each application, inside Google Play. Each application that Google removes in less than a month is considered PHAs.

This new approach allows us to create a new way of detection that avoids imitating the criteria and bias of antivirus engines and creates a unique machine learning model able to identify PHAs inside application markets. This machine learning model is able to detect applications whose characteristics are similar to PHAs that have been previously removed and present a lifespan of less than a month inside the Google Play Store Market.

On the other hand, the samples of non-malicious applications need to be filtered before their inclusion on the dataset. The reason for this is due to the fact that a large number of malware applications are not removed from the Google Play Store. This make necessary to verify that the samples collected are benign. All possible non-malicious applications have been verified through VirusTotal [46]. This service allows scanning each sample by 67 different antivirus engines, ensuring that all applications are harmless. Only applications with 0 detection rate and a period of life greater than six months have been included as non-malicious applications. The rest of the possible non-malicious applications were not included inside our dataset. Even though some of them present a low detection rate in VirusTotal we preferred to avoid those cases. The usage of VirusTotal service can seem counterproductive because we are involving antivirus detection bias in our dataset creation process. But like other security solutions, this new detection method need to maintain a False Negative (FN) ratio to the minimum. The usage of VirusTotal is only used to successfully guaranteed a clean dataset of legitimate applications. VirusTotal allow us the possibility of removing PHAs from the dataset, malicious applications with more than six months of life inside the Google Play Store. We look up to obtain a significant sample of legitimate applications and their lifespan, and if we only base on the number of downloads we could end tainting that sample. Several malicious campaigns have been known for being able to accomplish millions of downloads inside official markets during extended periods of time [47], [48]. We would have preferred not to depend on existing antivirus solutions in any part of the process. But this was the only option that allows us to obtain a legitimate dataset of applications published in the application markets. The usage of Tacyt guaranteed that these applications were published in the application market and the number of downloads but not its legitimacy. This classification process, previous to the training, is shown in Figure 1. In total, the dataset contains 91,203 applications, divided as shown in Table 1.

B. DATASET COVERAGE

Tacyt allows to query a database with more than seven million applications published inside the Google Play Store, and it

TABLE 1. Classification of application samples.

	Applications	Percentage
Malicious	36,539	40.06%
Benign	54,664	59.94%

also offers valuable metadata like the number of downloads of each application, publisher or market category amongst others. Based on that information a dataset has been created. The distribution based on downloads of Tacyt database can be found in Table 2. A distribution based on the number of downloads of each application ensures the representativity and coverage of the dataset. As mentioned before, our dataset is composed of [91,203] applications, a distribution based on the number of downloads of our dataset that is presented in Table 3.

If we compare Table 2 and Table 3 several differences can be appreciated. There is a larger number of applications in our dataset within the range of 201, 1000 downloads and less number of apps within the range of 10001, 100000 and 100001, 500000. To not unbalance the dataset we maintained a similar number of malicious and benign applications in our dataset. Due to our criteria for selecting malicious applications, an application with a lifespan less than a month inside the Google Play Store, it is not possible to find a lot of results with more than 10001 downloads. Because of this reason, we increased the range 201, 1000 to have more malicious applications.

TABLE 2. Distribution inside Tacyt database based on the number of downloads.

Download range	Population - Play Store Applications	Percentage
[0, 200]	2,686,557	39.40
[201, 1000]	1,089,295	15.98
[1001, 10000]	1,529,846	22.44
[10001, 100000]	980,316	14.38
[100001, 500000]	345,425	5.07
[500001, ∞]	186,832	2.73

TABLE 3. Distribution inside our dataset based on the number of downloads.

Download range	Population - Play Store Applications	Percentage
[0, 200]	35,935	39.40
[201, 1000]	31,016	34.00
[1001, 10000]	13,820	15.15
[10001, 100000]	7942	8.7
[100001, 500000]	505	0.55
[500001, ∞]	1985	2.17

Altogether, 601 features have been extracted from each application. These include the permissions requested by the application, the hardware resources that the application it is trying to access, and the information published on the Google Play Store. The entire dataset, that is composed of these features, is used to train and test the effectiveness of the learning model. Moreover, authors also considered Android run time permissions too. Starting with Android 6.0, Marshmallow, developers can ask for permissions on runtime. But those permissions need to be specified in the app's manifest file, like any other permission [49]. Tacyt extracts permissions using different techniques. One of them is the analysis of the app's manifest files, which guarantee the extraction of runtime and non-runtime permissions. This dataset is the one that allows us to create a new method for PHA detection that avoids the replication of existing antivirus engines and uses the lifespan as a feature. This novel method can detect with a 90% accuracy when an application is going to be removed, in a period less than a month, from the Google Play Store. Other research methods have presented better accuracy measurements but it is necessary to bring out again the differential characteristics of this novel method of detection. To the best of our knowledge, this is the first malware detection method that uses the lifespan of applications inside a market as selection and detection criteria.

To assure a representative and coverage of our dataset, the number of downloads is not the only metric that we checked. On one hand, we added and reviewed the number of android permissions used in our dataset. There are 455 permissions, which identify the data and system features that the applications may access.

Most declared permissions, by the applications stored in the dataset, are shown in Table 4.

TABLE 4. Most popular permissions in Android applications.

Permission	Applications	Percentage
INTERNET	88,850	0.97
ACCESS_NETWORK	84,848	0.93
READ_EXTERNAL_STORAGE	55,023	0.60
WRITE_EXTERNAL_STORAGE	54,576	0.41
WAKE_LOCK	37,391	0.41
ACCESS_WIFI_STATE	37,226	0.33
Others	Less than 30,000	-

On the other hand, hardware access permissions were included and then tested as representative attributes of the sample. These android permissions refer to the use of some hardware components, like the camera. All those hardware components of the Android operating system have been included in the dataset as characteristics of each application.

In total, 105 hardware declarations have been included in the dataset. Those declarations are distributed, as shown in Table 5, across the dataset.

Finally, data application size, price, minimum Android SDK version, and developer have been included as features.

TABLE 5. Most popular hardware components in Google Play Store applications.

Hardware	Applications	Percentage
Android.hardware.camera	762	0.8%
Android.software.live_wallpaper	326	0.4%
Android.hardware.screen.portrait	275	0.3%
Android.hardware.touchscreen	195	0.2%
Android.hardware.sensor.accelerometer	111	0.1%
Android.hardware.screen.landscape	100	0.1%

We considered this information useful in the detection of PHAs and also allowed us to get some insights about popular categories, like games or education applications. As an example of this, malware designed to act like small-sized video games may have different permissions and features than malware designed to act like medium-sized social applications. The category and type of each application, which determine how it is classified in the Google Play Store, is presented in Table 6.

TABLE 6. Most common categories on the Google Play Store.

Category	Applications	Percentage
ENTERTAINMENT	10,604	11.63%
GAME	7,399	8.11%
MUSIC_AND_AUDIO	6,164	6.76%
TOOLS	5,579	6.12%
BOOKS_AND_REFERENCE	5,556	6.09%
EDUCATION	5,131	5.63%
LIFESTYLE	5,080	5.57%

C. FEATURES SETS AND NORMALIZATION

This research has always taken into account the current situation and techniques of PHA development and distribution. This knowledge has been applied in the creation of the dataset and the following feature selection. The proposed solution is intended to be a real solution that can be applied to all possible Android applications, independently of the device manufacturer. As previously mentioned, the features selected for this training have been specifically studied and every feature that did not represent a common characteristic between applications has been removed. The solution proposed in this paper does not use network addresses, activity names or specific permissions associated with a manufacturer. Different PHAs will only share those features in the case that they are from the same family or developer. For example, in the case of botnets different PHAs will not share the same network addresses because they will have different command-and-control (C&C) servers. Involving these features will grant further detection rates in our test dataset but will not be representative of a real case scenario.

Moreover, multiple permissions may be the same but present differences based on the application package. Table 7 presents some Android permissions used in Drebin [37] and then normalized in our experiments. This process is the one that allows us to only use 601 features instead of thousands. It is necessary to make clear that this process was not designed to create a lightweight system but to create a generic solution that can behave well in real environments. The lightweights of the system is a consequence of this feature selection process. Regarding this topic, recent works have also tried to find the best features for machine learning training. Surendran *et al.*, used a system call sequence generated by malware applications to identify common patterns and create detection features [50]. The mentioned solution is a dynamic analysis solution, but any real applicable solution needs to involve a feature selection process and involve common features across multiple applications.

D. MACHINE LEARNING CLASSIFIERS

PHA automatic detection, like any other malware detection, is a binary classification problem. And supervised machine learning algorithms have proven to be successful detecting PHAs in numerous studies [27], [29], [32]. The use of mathematical algorithms oriented to classification problems allow the creation of trained models that sort out different applications based on their features. But it is necessary to take into account that the accuracy of these algorithms are heavily related to the training dataset. Using supervised training, all the data must be chosen carefully to obtain good performances. Our approach follows these ideas but with substantial changes like the selection and normalization of features and the dataset creation process.

Machine Learning algorithms search for a mathematical function that is able to distinguish effectively between different types of samples. Since this is a binary classification problem, and taking into account the current state of the art, the following algorithms have been chosen: Support Vector Machines(SVM), Stochastic gradient descent(SGD), Random Forest Classification(RFC) y eXtreme Gradient Boosting(XGB). Most research work uses SVM [30] or One-Class SVM algorithms [27] but we extended the test set involving RFC and a modern classifying algorithm like XGB. Those algorithms are the ones that have been used to train a model using our custom dataset. And later on, their effectiveness and accuracy in classifying PHAs have been exhaustively evaluated.

The training has been done gathering 70% of the samples randomly, 63,842 of 91,203. The remaining 30% is used as the test dataset, 27,361 of 91,203. Thus, the test dataset allows establishing the effectiveness of the generated model through the use of the metrics precision, recall, and f1-score.

The algorithms used are implemented on the Scikit-learn[2] and DMLC-XGBoost[3] libraries, both written in Python. Scikit-learn allows using a training method known as grid search. It searches for the most optimum parameters, of each Machine Learning algorithm, during the model training. The grid search looks for the parameters that achieve a better f1-score. We used f1-score as a measure of a test's accuracy because considers both the precision and the recall of the test to compute the score.

A more detailed and formal description of the machine learning process used during the training of the model are the following:

- Stochastic gradient descent (SGD) [51] algorithm used tries to minimize the value returned by the softmax function. It searches for a hyperplane that divides the dataset into two classes. The effectiveness of this model depends on whether the classes of the problem are linearly separable.
- Support vector machine (SVM) [52] algorithm has been widely used in classification problems.

[2] https://scikit-learn.org/stable/

[3] https://github.com/dmlc/xgboost

TABLE 7. Example of specific application permissions.

Permission	Normalized permission
com.samson.samsonproductions.**permission.C2D_MESSAGE**	permission.C2D_MESSAGE
com.dreamstep.wsmsanonymes.**permission.C2D_MESSAGE**	permission.C2D_MESSAGE
com.google.android.apps.chrometophone.**permission.C2D_MESSAGE**	permission.C2D_MESSAGE
com.android.samsung.rmt_exercise.**permission.KEYSTRING**	permission.KEYSTRING
com.sec.modem.settings.**permission.KEYSTRING**	permission.KEYSTRING

The implementation used in this research base its classification function on a Gaussian kernel. Thus, it is able to effectively distinguish radially separable problems.

- Random Forest Classification (RFC) [53] algorithm creates different sets of random decision trees. Through the training, it chooses the set whose decision trees make better decisions on average.
- eXtreme Gradient Boosting [54], [55] algorithms are used in classification [56] to create prediction models based on an ensemble of weak prediction models. Those weak models are decision trees that, through the training, discard the less valuable features of a certain data class. The most valuable features create decision trees with an associated weight. The total sum of these weights is the output value that identifies each class. This behaviour allows an application, depending on whether its category is Tools or Education, to be classified in a different way even when their features are similar.

IV. RESULTS

A. MACHINE LEARNING MODELS TRAINING AND COMPARISON

Due to the balanced dataset, distribution and the normalized features, we expected that novel optimized gradient boosting classifiers like XGBoost outperform other traditional classifiers like SVM. Results for the SGD are presented on Table 8. SGD returned 13,809 as true negatives samples, 8,929 as true positive, 2,183 as false negatives and 2,440 false positive samples, resulting in an overall f1-score score of 83%.

TABLE 8. SGD Classification Report.

Dataset	Precision	Recall	f1-score
Goodware	86%	85%	86%
Malware	79%	80%	79%
Average	83%	83%	83%

Results for the SVM are presented on Table 9. SVM returned 13,748 as true negatives samples, 8,816 as true positive, 2,101 as false negative and 2,696 false positive samples, resulting in an overall f1-score score of 83%.

TABLE 9. SVM Classification Report.

Dataset	Precision	Recall	f1-score
Goodware	87%	84%	85%
Malware	77%	81%	79%
Average	83%	82%	83%

Results for the RFC are presented on Table 10. RFC returned 15,311 as true negatives samples, 9,222 as true positive, 1,487 as false negative and 1,341 false positive samples, resulting in an overall f1-score score of 90%.

TABLE 10. RFC Classification Report.

Dataset	Precision	Recall	f1-score
Goodware	91%	92%	92%
Malware	87%	86%	87%
Average	90%	90%	90%

Results for the XGB are presented on Table 11. XGB returned 15,150 as true negatives samples, 9,316 as true positive, 1,648 as false negative and 1,247 false positive samples, resulting in an overall f1-score score of 89%.

TABLE 11. XGB Classification Report.

Dataset	Precision	Recall	f1-score
Goodware	90%	92%	91%
Malware	88%	85%	87%
Average	89%	89%	89%

Table 12 presents the results of different machine learning algorithms applied to our dataset. Even though the model trained with the XGB algorithm reaches 89% accuracy, the RFC model achieves 90% accuracy with a false positive rate of 5.43%. It is a small difference, but it made RFC the suited algorithm for this problem. A greater difference was found in the models trained with SVM and SGD, achieving an 82% and an 83% of f1-score respectively. This denotes the fact that algorithms based on ensemble learning are the best ones facing this type of problems.

TABLE 12. Comparison of different classification algorithms.

Algorithm	Precision	f1-score	False negative	False positive
SVM	83%	83%	7.98%%	8.92%
SGD	83%	83%	7.68%	9.85%
RFC	90%	90%	5.43%	4.01%
XGB	89%	89%	6.03%	4.56%

V. DISCUSSION

After the training, the results obtained seem to be promising. On one hand, we have XGB with an accuracy of 89% and on the other hand, we have RFC with a 90% accuracy.

SVM and SGD did not behave that well with our dataset in comparison with RFC. This has some explanation, since the classification of malware and PHAs are not always a simple task. It is difficult to draw a line between the different sets of applications. Like we mentioned before in this paper this is also shown in the antivirus market [21]. Some applications could be PHAs to some antivirus engines and others could be considered non-malicious applications by other antivirus engines. In a malware classification problem, we will always encounter a lot of grey areas.

Because of that difficult classification, a random forest approach behaves better selecting malware and PHAs applications. Also, the RFC algorithm allows us to identify which features are more important when classifying samples. Using the 601 features, which constitute the dataset, those with more weight are shown in Table 13.

TABLE 13. Most important features.

Feature	Importance
applicationType (APPLICATION)	0.159357
targetSdkVersion	0.090245
nFiles	0.083069
size	0.078786
minSdkVersion	0.066245
nActivities	0.050453
nImages	0.049002
nPermissions	0.032027
Other features	0.388817

Previous research like Drebin had achieved an accuracy of 93.90% [30], but they do not present other values like recall, precision, or f1-score. Furthermore from our point of view, Drebin did not apply a generic approach to features selection. They present a solution with 545,000 different features. Like mentioned before Drebin uses network addresses, activities' names, and other unique features. Because of the large quantity and type of features selected it will not behave well in a real world environment. These unique features has been taken into account, features that will only exist in an application of a group of applications developed by the same developer or group of developers.

If you use network addresses as a feature you will detect some PHAs but you will discard others inside the model because that feature will not be present in all cases. To detect the error inserted by these features, it will be necessary to evaluate the weight of each feature inside the model.

The proposed model uses 601 features. This is a great difference and it generates a lightweight machine learning system, in comparison with other works like Drebin that instead has used 545,000 [37] features. Sometimes the reduction of features could have an impact on the accuracy. But research works like Cai *et al.* has shown that a specific set of selected features, in their work they only used 70 features, can obtain promising results in PHAs detection [41]. Moreover, it is necessary to take into account that all of the 601 features selected could exist in any Android application. Because of this selection of features, we consider that our approach will present better results in a real world environment. Additionally the lightweight of the system directly affect the MTTD of the system. A PHA can be identified in less than a second by the system. Like any other machine learning system, the system will need to periodically be retrained but this factor also affects this timing. The lightweight of the system reduces the amount of time and hardware needed to train this solution.

All these results can be summarized in two main contributions. First, that it is possible to use methods based on the lifespan of applications inside Google Play Store, for creating PHAs datasets. And second, the number of features required for training these machine leanings models have been drastically reduced, 601 versus other machine learning systems that used thousands of features [37], [44].

Moreover, it could be interesting to compare these results with other industries and research solutions, not only previous research papers. The industry average is around 98%, according to the studies of AV-TEST - The Independent IT-Security Institute [57]. But it is necessary to take into account that these solutions also perform dynamic analysis of the applications, the presented solution is only based on static analysis features. Another comparison can be made against Google Play Protect, the mobile malware detection solution offered by Google. This solution has an accuracy of around 70% [10] analyzing applications published in the Google Play Store.

A. REAL-TIME USE CASE SCENARIO

Through the different sections of this paper, we have mentioned how this system has been designed to be applied in a real use case scenario. The design and test have always taken this into account. The proposed way to use this machine learning detection system in the real world could be to use it as an application validation process.

Before the publishing of an Android application into any store, this application can be scanned by the machine learning system presented in this paper. Being an automatic process it will not severely impact the application validation process. Thus, this validation can be used as an indicator of PHA. The current machine learning model present a MTTD (Mean Time To Detect) smaller than one second per application. Being a static analysis method, it does not need to study the application behaviour for a specified amount of time inside a sandbox. This MTTD could be increased if the feature extraction time is taken into account. In order to evaluate the application through this system, the application's permissions, accessed hardware components and categories to publish need to be known. Most of this information is available in the Android application manifest, so collection time must be considered. And even though that the process of obtaining and parse an Android application manifest can be done in a matter of seconds, any official application store can ask for this information. During the upload and submission process of an application, the application market can ask for a separate manifest file, corresponding to the application, in the submission form. In conclusion, the small MTTD would not affect the submission performance of applications and will end blocking several PHA along the process.

On the other hand, one of the problems of this system will be with the False Negative rate, 5,43%, but further work and data could improve this detection rate.

VI. CONCLUSION AND FUTURE WORK

This paper presents a new way for training and detecting PHAs inside the Android ecosystem. The objective is to detect mobile applications that will be removed by Google in a period shorter than one month, where applications removed by Google in short periods from the store are, in most cases, PHAs or malware. To achieve this goal, a new dataset has been created and several classification algorithms have been used, SGD, SVM, RFC, and XGB. The dataset creation uses as criteria the lifespan of an application inside Google Play instead of antivirus decision engines, for identifying PHAs. Training with this dataset a Random Forest Classifier machine learning, a 90% of effectiveness can be reached.

One of the main limitations of this approach is its accuracy. Future work can be done in this aspect and for example, the combination of several algorithms through ensemble learning techniques could obtain better results. Also, like any other machine learning model, it is necessary to periodically retrain this detection model with new data to detect new threats.

Another possible limitation is the way that PHAs are selected in our dataset. The proposed approach considered PHAs based on the lifespan of applications inside the Google Play Store. Our selected PHAs are applications that Google banned or removed from the Google Play Store. But it is not possible to know how many of them were PHAs or applications infringing Google Play Store policies. Applications could not be a PHA but Google could consider that it is infringing publishing policies. Moreover, a lot of PHAs are not banned or retired by Google in a short period. Our machine learning model is detecting the most common and aggressive campaigns but most elaborated ones could evade our system.

Finally, this approach has proved that is possible to create an automated analysis solution for detecting PHAs based on the lifespan of the application inside markets. On one hand, Google could use this system to detect if a new application is going to be removed from the Google Play Store and use it as a filter for newly published applications. On the other hand, any security research could use this model for detecting aggressive mobile malware campaigns. Finally, we also prove that a limited set of generic features can be used for detecting PHAs.

These results also evidence the necessity of identifying and conceiving new detection methods that avoid the usage of antivirus commercial models. To increase detection rates new methods that do not try to emulate actual commercial tools need to be developed.

REFERENCES

[1] *Mobile Operating System Market Share Worldwide*. Accessed: Jun. 11, 2021. [Online]. Available: https://gs.statcounter.com/os-market-share/mobile/worldwide

[2] G. Kelly. (2014). *Report: 97% of Mobile Malware is on Android. This is the Easy Way You Stay Safe*. [Online]. Available: https://www.forbes.com/sites/gordonkelly/2014/03/24/report-97-of-mobile%-malware-is-on-android-this-is-the-easy-way-you-stay-safe

[3] C. Lueg. (Jun. 2017). *8, 400 New Android Malware Samples Every Day*. [Online]. Available: https://www.gdatasoftware.com/blog/2017/04/29712-8-400-new-android-malw%are-samples-every-day

[4] (2020). *Smartphone Users*. [Online]. Available: https://www.statista.com/statistics/330695/number-of-smartphone-users-w%orldwide/

[5] J. H. Says. (Jan. 2020). *SMiShing: About the FedEx SMS Phishing Scam | McAfee*. [Online]. Available: /blogs/consumer/consumer-threat-notices/fedex-sms-phishing-scam/

[6] J. H. Says. (Jan. 2020). *SMiShing: About the FedEx SMS Phishing Scam | McAfee*. [Online]. Available: /blogs/consumer/consumer-threat-notices/fedex-sms-phishing-scam/

[7] *FakeSpy Android Malware Spread Via Postal-Service Apps*. Accessed: Jun. 11, 2021. [Online]. Available: https://threatpost.com/fakespy-android-malware-spread-via-postal-servic%e-apps/157102/

[8] P. Kotzias, J. Caballero, and L. Bilge, "How did that get in my phone? Unwanted app distribution on Android devices," 2020, *arXiv:2010.10088*. [Online]. Available: http://arxiv.org/abs/2010.10088

[9] Statista. (2017). *Number of Available Applications in the Google Play Store From December 2009 to December 2020*. [Online]. Available: https://www.statista.com/statistics/266210/number-of-available-applicat%ions-in-the-google-play-store/

[10] *Test Google Play Protect 24.3 for Android (213208)*. Accessed: Jun. 11, 2021. [Online]. Available: /en/antivirus/mobile-devices/android/march-2021/google-play-protect-24.%3-213208/

[11] MalwareBytes. (Mar. 2018). *Android Security 2017 Year in Review*. [Online]. Available: https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf

[12] S. Hutchinson, B. Zhou, and U. Karabiyik, "Are we really protected? An investigation into the play protect service," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2019, pp. 4997–5004.

[13] D. Maier, T. Müller, and M. Protsenko, "Divide-and-conquer: Why Android malware cannot be stopped," in *Proc. 9th Int. Conf. Availability, Rel. Secur.*, Sep. 2014, pp. 30–39.

[14] BleepingComputer. (Nov. 2017). *Google Play Store Sees Sudden Surge of Malicious Apps*. [Online]. Available: https://www.bleepingcomputer.com/news/security/google-play-store-sees-s%udden-surge-of-malicious-apps/

[15] MalwareBytes. (Nov. 2017). *New Android Trojan Malware Discovered in Google Play*. [Online]. Available: https://blog.malwarebytes.com/cybercrime/2017/11/new-trojan-malware-dis%covered-google-play/

[16] Y. Zhou, Z. Wang, W. Zhou, and X. Jiang, "Hey, you, get off of my market: Detecting malicious apps in official and alternative Android markets," in *Proc. NDSS*, vol. 25, no. 4, Feb. 2012, pp. 50–52.

[17] Techcrunch. (May 2018). *Google's Android Things IoT Platform Comes Out of Beta*. [Online]. Available: https://techcrunch.com/2018/05/07/googles-android-things-iot-platform-c%omes-out-of-beta/

[18] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "IoT security: Ongoing challenges and research opportunities," in *Proc. IEEE 7th Int. Conf. Service-Oriented Comput. Appl.*, Nov. 2014, pp. 230–234.

[19] R. Kumar, X. Zhang, W. Wang, R. U. Khan, J. Kumar, and A. Sharif, "A multimodal malware detection technique for Android IoT devices using various features," *IEEE Access*, vol. 7, pp. 64411–64430, 2019.

[20] Z. Ren, H. Wu, Q. Ning, I. Hussain, and B. Chen, "End-to-end malware detection for Android IoT devices using deep learning," *Ad Hoc Netw.*, vol. 101, Apr. 2020, Art. no. 102098. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870519310984

[21] I. Gashi, V. Stankovic, C. Leita, and O. Thonnard, "An experimental study of diversity with off-the-shelf AntiVirus engines," in *Proc. 8th IEEE Int. Symp. Netw. Comput. Appl.*, Jul. 2009, pp. 4–11.

[22] M. Hurier, K. Allix, T. F. Bissyandé, J. Klein, and Y. Le Traon, "On the lack of consensus in anti-virus decisions: Metrics and insights on building ground truths of Android malware," in *Detection of Intrusions and Malware, and Vulnerability Assessment* (Lecture Notes in Computer Science), J. Caballero, U. Zurutuza, and R. J. Rodríguez, Eds. Cham, Switzerland: Springer, 2016, pp. 142–162.

[23] A. Mohaisen, O. Alrawi, M. Larson, and D. McPherson, "Towards a methodical evaluation of antivirus scans and labels," in *Proc. Int. Workshop Inf. Secur. Appl.*, USA. Cham, Switzerland: Springer, Aug. 2013, pp. 231–241.

[24] D. J. Sanok, Jr., "An analysis of how antivirus methodologies are utilized in protecting computers from malicious code," in *Proc. 2nd Annu. Conf. Inf. Secur. Curriculum Develop.* Kennesaw, GA, USA: Kennesaw State Univ., Sep. 2005, pp. 142–144.

[25] C. Willems, T. Holz, and F. Freiling, "Toward automated dynamic malware analysis using CWSandbox," *IEEE Secur. Privacy*, vol. 5, no. 2, pp. 32–39, Mar./Apr. 2007.

[26] L. K. Yan and H. Yin, "Droidscope: Seamlessly reconstructing the $*OS*$ and Dalvik semantic views for dynamic Android malware analysis," in *Proc. 21st USENIX Secur. Symp. (USENIX Secur.)*, 2012, pp. 569–584.

[27] J. Sahs and L. Khan, "A machine learning approach to Android malware detection," in *Proc. Eur. Intell. Secur. Informat. Conf.*, Aug. 2012, pp. 141–147.

[28] Z. Yuan, Y. Lu, Z. Wang, and Y. Xue, "Droid-sec: Deep learning in Android malware detection," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 4, pp. 371–372, 2014.

[29] J. Li, L. Sun, Q. Yan, Z. Li, W. Srisa-An, and H. Ye, "Significant permission identification for machine-learning-based Android malware detection," *IEEE Trans. Ind. Informat.*, vol. 14, no. 7, pp. 3216–3225, Jul. 2018.

[30] D. Arp, M. Spreitzenbarth, M. Hubner, H. Gascon, K. Rieck, and C. Siemens, "DREBIN: Effective and explainable detection of Android malware in your pocket," in *Proc. NDSS*, vol. 14, 2014, pp. 23–26.

[31] I. Martín, J. A. Hernández, A. Muñoz, and A. Guzmán, "Android malware characterization using metadata and machine learning techniques," *Secur. Commun. Netw.*, vol. 2018, pp. 1–11, Jul. 2018.

[32] N. Peiravian and X. Zhu, "Machine learning for Android malware detection using permission and API calls," in *Proc. IEEE 25th Int. Conf. Tools With Artif. Intell.*, Nov. 2013, pp. 300–305.

[33] B. Baskaran and A. Ralescu, "A study of Android malware detection techniques and machine learning," presented at the Mod. Artif. Intell. Cogn. Sci. Conf. Dayton, OH, USA: Univ. Dayton, Apr. 2016, p. 9. [Online]. Available: https://ecommons.udayton.edu/maics/2016/Saturday/3/

[34] K. A. Talha, D. I. Alper, and C. Aydin, "APK Auditor: Permission-based Android malware detection system," *Digit. Invest.*, vol. 13, pp. 1–14, Jun. 2015.

[35] R. Kumar, X. Zhang, R. U. Khan, and A. Sharif, "Research on data mining of permission-induced risk for Android IoT devices," *Appl. Sci.*, vol. 9, no. 2, p. 277, Jan. 2019. [Online]. Available:https://www.mdpi.com/2076-3417/9/2/277

[36] R. Kumar, W. Wang, J. Kumar, T. Yang, and W. Ali, "Collective intelligence: Decentralized learning for Android malware detection in IoT with blockchain," 2021, *arXiv:2102.13376*. [Online]. Available: http://arxiv.org/abs/2102.13376

[37] Drebin. *Drebin Dataset*. Accessed: Nov. 9, 2017. [Online]. Available: https://www.sec.cs.tu-bs.de/~danarp/drebin/

[38] F. Wei, Y. Li, S. Roy, X. Ou, and W. Zhou, "Deep ground truth analysis of current Android malware," in *Proc. Int. Conf. Detection Intrusions Malware, Vulnerability Assessment (DIMVA)*. Bonn, Germany: Springer, 2017, pp. 252–276.

[39] W. Li, X. Fu, and H. Cai. (Jan. 2021). *AndroCT: Ten Years of App Call Traces in Android*. Type: Dataset. [Online]. Available: https://zenodo.org/record/5010831

[40] H. Cai. (Jan. 2020). *TraceDroid: Eight-Year Behavioral Profiles of Android Apps*. Type: Dataset. [Online]. Available: https://zenodo.org/record/3665877

[41] H. Cai, N. Meng, B. G. Ryder, and D. Yao, "DroidCat: Effective Android malware detection and categorization via app-level profiling," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 6, pp. 1455–1470, Jun. 2019

[42] H. Cai and B. G. Ryder, "A longitudinal study of application structure and behaviors in Android," *IEEE Trans. Softw. Eng.*, early access, Feb. 19, 2020, doi: 10.1109/TSE.2020.2975176.

[43] H. Cai, X. Fu, and A. Hamou-Lhadj, "A study of run-time behavioral evolution of benign versus malicious apps in Android," *Inf. Softw. Technol.*, vol. 122, Jun. 2020, Art. no. 106291. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0950584920300410

[44] Q. Han, V. S. Subrahmanian, and Y. Xiong, "Android malware detection via (somewhat) robust irreversible feature transformations," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3511–3525, 2020.

[45] Q. Wu, M. Li, X. Zhu, and B. Liu, "MVIIDroid: A multiple view information integration approach for Android malware detection and family identification," *IEEE MultimediaMag.*, vol. 27, no. 4, pp. 48–57, Oct. 2020.

[46] VirusTotal. *Virustotal. Free Online Virus, Malware and URL Scanner*. Accessed: Oct. 5, 2019. [Online]. Available: https://www.statista.com/statistics/274774/forecast-of-mobile-phone-use%rs-worldwide/

[47] (Oct. 2019). *Google Play Store Malware Hits 42 Apps With 8 Million Downloads*. [Online]. Available: https://www.digitaltrends.com/mobile/google-play-store-malware-hits-42-%apps-with-8-million-downloads/

[48] D. Winder. *New Android App Malware Infects 250 Million Downloads–Here's What You Need to Know*. Section: Cybersecurity. Accessed: Oct. 5, 2019. [Online]. Available: https://www.forbes.com/sites/daveywinder/2019/03/13/new-android-app-mal%ware-infects-250-million-downloads-heres-what-you-need-to-know/

[49] *Request App Permissions*. Accessed: Jul. 19, 2021. [Online]. Available: https://developer.android.com/training/permissions/requesting

[50] R. Surendran, T. Thomas, and S. Emmanuel, "On existence of common malicious system call codes in Android malware families," *IEEE Trans. Rel.*, vol. 70, no. 1, pp. 248–260, Mar. 2021.

[51] H. Robbins and S. Monro, "A stochastic approximation method," in *The Annals of Mathematical Statistics*. USA, 1951, pp. 400–407.

[52] T. Fletcher, "Support vector machines explained," Tutorial Paper, 2009, pp. 1–19. [Online]. Available: https://d1wqtxts1xzle7.cloudfront.net/43282568/SVM_Explained-with-cover-page-v2.pdf?Expires=1629968616&Signature=LRvcm2bJ4ipySw~14j4sls6wz-kCVwLIGAq2CiUMryiUE30Xe8waIIAckZHGVEXVUBPcSaSJO4eHyFwIxbbv2SzFNcqdYlqtZLHHaaYhiQjlAJXQRc7MTRC8pmFibCBNvbNaGmnHsiOLn-m9QDFXQya3SXufPq5CJ9kqE6eC5Jtu4gaTuqSfga1RgSgtgprkpRRd6V9eTLr9kjlcQMzzN1Y2vvajIN5i6Fov-buE8CxRWIVt59e8c6zhIst wA1mXYJFiUHHbR2vayaP2N4mu7KmvAt7xdugozURHtLlKq9zU3WxKL28lacQEVVFWYr20w6MnqjgFmbNh-yspFDFcg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

[53] L. Breiman, "Random forests," *Mach. Learn.*, vol. 45, no. 1, pp. 5–32, 2001, doi: 10.1023/A:1010933404324.

[54] J. H. Friedman, "Greedy function approximation: A gradient boosting machine," *Ann. Statist.*, vol. 29, no. 5, pp. 1189–1232, Oct. 2001.

[55] J. H. Friedman, "Stochastic gradient boosting," *Comput. Statist. Data Anal.*, vol. 38, no. 4, pp. 367–378, 2002.

[56] I. B. Mustapha and F. Saeed, "Bioactive molecule prediction using extreme gradient boosting," *Molecules*, vol. 21, no. 8, p. 983, 2016.

[57] (2021). *Test Antivirus Software for Android*. Accessed: Jul. 19, 2021. [Online]. Available: https://www.av-test.org/en/antivirus/mobile-devices/

2.3 Summary of the results of Article 1

In this chapter, a detection method of PHAs based on lifespan measurements has been shown. This method is based on machine learning techniques that use lifespan measurement and other common features of apps published on the Google Play Store. Unique features like the usage of a certain IP address have not been used in the training, designing a heterogeneous solution. Moreover, one of the great differences of this article, compared to other publications [75][31], is the avoidance of usage of antivirus engines. The criterion for the selection of applications was their lifetime, being apps with a lifespan greater than six months legitimate and apps removed by Google in a period of less than a month were considered PHAs. This approach proved to be valid after several tests. Thus machine learning techniques are applicable and proved successful in this research. Also, being a solution that can be deployable in app markets can cover and improve the security of all android mobile vendors. Any app market can apply this detection technique as a filtering method for new applications.

After the study and experimentation of machine learning techniques applicable to PHAs detection, several questions remained on the table. Detection methods are needed because multiples attacks against the healthcare industry are happening [76][77] but what is the focus of these attacks? Some cyberattacks may be aimed at disrupting critical services, but several of them are centred on stealing medical information [78]. Reaching this point, another question is how this medical information was being sold and where. In the next chapter, an analysis of darknets will be presented and their usage as a method of selling stolen information will be studied.

Chapter 3

Analysis of darknets and their connections

3.1 Paper 2 contribution

Sell stealing information has always been a way of monetizing cyberattacks [79]. There are certain types of information that are extremely valuable (e.g, passwords, phone numbers or social security numbers). For example, passwords can be useful to perform new attacks, due to the fact that people reuse passwords [80] , phone numbers can be used in smishing campaigns [80] and social security numbers can be use to stole identities [81] Unfortunately, healthcare data presents all previously mentioned types of information and more. Because of that, healthcare data, such as Electronic health records (EHR), is particularly interesting to cybercriminals [50].

One of the most popular ways, used by cybercriminals, of selling stolen information is the usage of darknets [82]. Darknets [13], also known as alternative or overlay networks, are a type of network focused on offering anonymity to its users. These darknets are built-in on top of the Internet and look to offer a way of accessing online content anonymously. Most of these networks also allow the creation of web services, such as webpages, where any content can be placed anonymously. The anonymity offered by those networks has led to the creation and offering of illegal services, being actively used by cybercriminals. For example, there are markets, known as dark markets, centred on offering illegal services (e.g, hacking services), products (e.g, drugs) or stolen data (e.g, credit card number or social security numbers) [83].

The most popular of these darknets is "The Onion Router" (Tor) [84][15] but there are other networks such as the "Invisible Internet Project" (i2p) [85]. Moreover, at the moment of writing this thesis, there are multiple active dark markets. The development of these privacy-oriented technologies also generates the problem of how to analyse and identify those dark markets. Unlike, the traditional Internet, darknets do not offer powerful search engines such as Google. Some attempts has been done into create and index darknet information [86][87]. But all freely accessible search engines present outdated information, and usually only present Tor network-related data.

Being this the situation, and looking for stealing healthcare data. As a part of this thesis, I collaborated on the creation of a tool capable of obtaining information from darknets. Crawl and index information from the darknet allows the detection of dark markets and leaks of information, among other valuable threat intelligence data.

In this chapter, we will address how to obtain information from two of the most popular darknets, Tor and i2p. And how in this process of obtaining information from both networks, it was discovered their interconnection. Finally, in the conclusions an analysis of the consequences and implications for the health sector will be presented.

3.2 Paper 2

The second scientific paper is included below, “Interconnection Between Darknets”.

Interconnection Between Darknets

Carlos Cilleruelo, Luis de-Marcos, Javier Junquera-Sánchez, and Jose-Javier Martínez-Herráiz, *Universidad de Alcalá, 28805 Alcalá de Henares, Spain*

Tor and i2p networks are two of the most popular darknets. Both darknets have become an area of illegal activities highlighting the necessity to study and analyze them to identify and report illegal content to law enforcement agencies (LEAs). This article analyzes the connections between the Tor network and the i2p network. We created the first dataset that combines information from Tor and i2p networks. The dataset contains more than 49k darknet services. The process of building and analyzing the dataset shows that it is not possible to explore one of the networks without considering the other. Both networks work as an ecosystem and there are clear paths between them. Using graph analysis, we also identified the most relevant domains, the prominent types of services in each network, and their relations. Findings are relevant to LEAs and researchers aiming to crawl and investigate i2p and Tor networks.

Over the last years, the exploration of the darknets has become of great importance for governments and law enforcement agencies (LEAs).[1] Even though the term darknet may refer to different things, it represents the space of the Internet that has been hidden by design,[2] through encryption or different routing overlapped technologies.

"The Onion Router" (https://www.Torproject.org/) (Tor) is the most popular technology of the darknet. Tor has been audited and investigated numerous times.[3–5] Tor has over 2 000 000 daily users and more than 6000 relays. (Tor Metrics: https://metrics.torproject.org/) Relays ensure that the network works, and they provide the privacy of the Tor network. The number of existing relays suggests significant support by an active community around this darknet. Another important feature of Tor is that it is possible to create websites and services called hidden services. Hidden services can only be accessed if we are connected to the Tor network. The original principle of Tor's hidden services was to avert censorship and facilitate freedom of speech. However, these hidden services have also turn into a space for criminal activity, like drug trafficking.[6] Tor popularity increased even more since it can also be used to offer anonymity in operating systems, like Tails. Tails became famous since Edward Snowden recommended using it (https://twitter.com/snowden/status/941018955405242369).

The second larger darknet is the "Invisible Internet Project,"(https://geti2p.net/) i2p. Like Tor hidden services, i2p offers eepsites, which are the websites and services available in this darknet. There are no public stats about daily users and services, but i2p is frequently maintained and developed. Also, like Tor hidden services, eepsitees became a place for illegal activities.[7,8]

To fight illegal activities, LEAs need techniques to discover, investigate, and correlate data between darknets. This article reports the research and tools for exploring Tor and i2p. We started developing tools for Tor like crawlers and scanners of hidden services. Initial exploration returned numerous references to eepsites. These references lead us to a second phase where we developed new tools to crawl and discover i2p, which also returned references to Tor hidden services sites. Crawling both darknets in parallel also provides more information, because crawlers get feedback from the other darknet. We found 8148 references to i2p eepsites from Tor hidden services and 487 Tor hidden services domains inside i2p eepsites. The information gathered by these tools was used to create a dataset of domains from both darknets and their connections, which provides a map of the darknet. Using graph analysis techniques, we further analyzed the connections between both darknets, and

1089-7801 © 2020 IEEE
Digital Object Identifier 10.1109/MIC.2020.3037723
Date of publication 11 December 2020; date of current version 18 June 2021.

also identified the most relevant actors and types of services offered by each network.

The main objective of this article is to analyze the interconnection between i2p and Tor, demonstrating the necessity to crawl both networks to get and to study the structure of the darknet and its services. Since the development of Tor and i2p networks is beyond the scope of this article, the following sections describe the creation of the dataset, the methodology to analyze the graph of the network, the results, and the implications for LEAs. The contributions of this article are summarized as follows.

- A dataset combining i2p and Tor crawled domains and their connections. Connections include links to any domain from both darknets. To our best knowledge, this is the first public dataset reporting i2p domains and also reporting domains from both networks. The dataset is publicly accessible in GitLab, https://gitlab.com/ciberseg-uah/interconection-between-darknets-dataset.
- A mapping of the darknet that covers a significant part of it.
- A rank of the most relevant domains in the darknet in terms of their position and influence, which shows that each darknet plays a different role offering specific services, and emphasizes the necessity to crawl and study one darknet to find sites in the other.

BACKGROUND

There are several studies that report the crawling,[2,9] discovery,[10] and dataset creation[11] for the Tor network. Also, several approaches focus on hybrid crawling,[12] searching for data in Tor, i2p, and Freenet. Most of the existing research tries to identify threat intelligence information and other critical information. The approach followed in this article is based on graph analysis to map the darknets. Our purpose is to evidence the connections between darknets and identify the relevant sizes and services that relate both darknets. To do that, we represent Tor and i2p as a directed graph and we apply graph analysis to measure the interdependence between networks and the position of individual domains.

Graph theory is useful to analyze social networks [13]. Furthermore, existing studies use graph analysis to investigate the Tor darknet.[11,14] This study uses graph analysis to identify relevant hidden services, eepsites, and to study the connection between the Tor and i2p.

In our work, the detection of influential nodes is done by analyzing the connections between them. This analysis was performed merging the data from i2p and Tor hidden services in a single dataset.

DASASET OF I2P AND TOR DOMAINS

In order to study the connections between Tor and i2p, we started by building a dataset of domains and relations. It stores which domain links to others. This returns a dataset that represents a network to study, through graph analysis, the interconnection between darknets.

At the moment of writing this article, there is not a public dataset with data from i2p and Tor network. We present here the first dataset with domains from i2p and Tor network. The dataset contains 49 249 domains (2687 domains from i2p and 46562 domains from Tor) and 304673 relationships between domains. There are datasets and collections of darknet domains like Ahmia dataset (https://ahmia.fi/) or DUTA-10k.[11] Lists of domains can also be found in popular websites like Pastebin and Reddit. However, none of them contains relationships between i2p and Tor domains. A comparison of the size of our dataset with existing ones returns that DUTA-10K has 10k onion domains compared >46k of our dataset. These figures do not include the fact that our dataset contains i2p domains too.

However, it is not possible to compare data of i2p since, at the moment of writing this, there are no public datasets. We can compare and check our data with Pastebin and Reddit domain lists, and our list of i2p domains turns out to be larger. Furthermore, an estimation of the number of i2p eepsites is difficult to find in academic literature.

Dataset Creation

To create the dataset and obtain all the possible information, we combined different approaches: using open-source lists of domains, crawling darknet sites, generating and verifying new domains, and deploying a modified relay in Tor.

First, we collected lists of hidden services and eepsites from open sources. There are many domains indexed in open sources like Pastebin or Reddit. Initially, we got the domains from these open sources manually, and then we developed automatic tools to perform this task.

An additional approach to obtain new domains is crawling the darknets. The specific details concerning how the crawler work is out of the scope

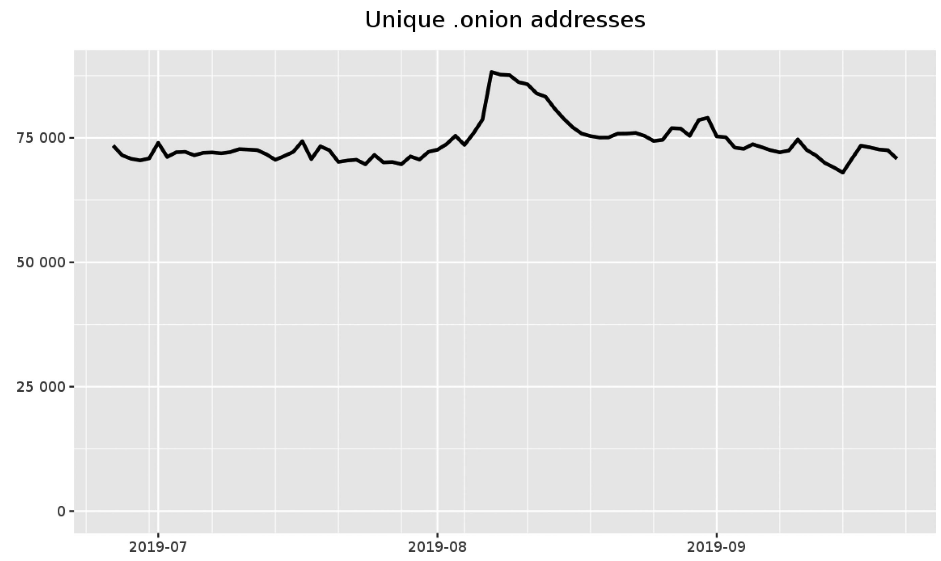

FIGURE 1. Onion services in 2019. Source: metrics.torproject.org (under Creative Commons Attribution 3.0 License - CC BY 3.0 US).

of this article, but we provide a short description. We built a crawler similar to the Ahmia project. Our crawling process started with the Hidden Wiki, (http://zqktlwi4fecvo6ri.onion) and explored recursively the links found there. After that, we improved the crawler for exploring and storing i2p eepsites. We used a similar approach to crawl i2p. Initially, we browsed i2p eepsites that list services. Using this crawling process, we obtained most of the data of our i2p/Tor dataset.

It is possible to take advantage of how Tor works to implement another two approaches: domain generation and modification of a Tor relay. Tor provides the possibility of domain generation using known words. A few hidden services need to be easily identified, so they generate domain names using keywords. For example, hidden services focused on selling drugs may try to generate domains with the words *drug* or *market* inside their domain name. In order to find more Tor domains, we developed a program that generated Tor domains with commonly used keywords. This program also checked if the domain is registered in the Tor network.

Tor relay modification is useful because Tor network structure does not have a public DNS server, it uses a service called Hidden Service DirecTory (HSDir). Some Tor relays are categorized with the flag HSDir. This means that they store information about hidden services. To obtain more valid Tor domains, we deployed a modified Tor relay and got the HSDir flag. This technique was previously reported in.[15] We edited the source code of the Tor relay to store hidden service descriptors that identify Tor domains. This technique is key to complete the dataset since it unveils domains that are not published on indexes or linked to other websites.

Dataset Coverage

The process to create the dataset took two years and used the combination of methods previously described. We also combined the results of the i2p and Tor crawling, allowing us to get more domains. We argue that is the reason for which we obtained substantially more domains than DUTA-10k dataset. The dataset stored the cross-relationships between i2p and Tor. In total, 487 relationships in our dataset are references from i2p eepsites to Tor hidden services, and there are 8148 references to eepsites in different Tor hidden services. Even though we gathered i2p and Tor domains for a long time, it is necessary to consider the coverage of the dataset.

We can estimate the coverage of our dataset by comparing it with the Tor network (https://metrics.torproject.org/). The Tor project states that there are around 75k unique onion services in 2019 (see Figure 1).

If we compare 75k with the >46k onion domains from our dataset, we estimate that it covers around 61% of the Tor network. However, it is necessary to point out that not all of these hidden services will be websites and that the domains of the dataset may go offline at any moment. Because of this, it is difficult to estimate the exact coverage of Tor darknet, despite the fact that our dataset contains more domains than other investigations.

Something similar happens if we try to estimate the coverage of the i2p network for our dataset. i2p does not provide official metrics. Although it maintains several updated indexes of domains, many eepsites are published in jump sites and public indexes. Also, as we mentioned before, there is no public i2p dataset of eepsites or research about i2p size or dimension, making difficult to estimate the coverage of i2p of our dataset.

METHODOLOGY

Graph Construction

The dataset was used to build a directed graph that represented the network. Nodes represent domains, and edges represent links between domains. All nodes are darknet domains from i2p and Tor. Surface web domains are not included in the dataset and the graph, because our interest is to study the interconnection between darknets. Also, the graph does not include duplicated links (same source and same target), and domains that point to themselves (self-links) as our study focuses on the unweighted connections existing between different nodes.

Graph Analysis

Graph analysis is used to compute metrics of graphs, nodes, and their relationships. Many graph algorithms have their origins in social network analysis, so graphs are sometimes called networks. In this research, we use graph metrics to analyze and compare the darknets (i2p and Tor) and the connections between them. This study reports the following graph metrics: density, average path length, diameter, average degree, and the number of connected components. Density is the ratio of the number of edges present to the total possible number of edges. The average path length is the average distance of all nodes to all other nodes. Diameter is the largest shortest path that can be found between any two nodes in the graph. Average degree measures the average number of incoming and outgoing edges of all nodes. A connected component is a set of connected nodes where each node is reachable from any other node in the same set. The number of connected components is the number of sets that are connected in this way. If all nodes are connected, then the graph contains only one connected component. Similarly, if a node is isolated having no edges to any other node, then it forms a component of just one node.

Node metrics are used to identify the most important nodes in the darknet. This study reports the following node metrics: degree, closeness centrality, betweenness centrality, and PageRank. Degree is an indicator of the popularity of individual nodes that measures the number of incoming and outgoing links in each node. As both numbers can be different in a directed graph, we distinguish between in-degree and out-degree. Closeness centrality measures the average inverse distance to all other nodes. Higher values of closeness centrality imply shortest distances to all other nodes. Nodes with a high closeness centrality can spread the information very efficiently through the graph. In this study, we use harmonic closeness centrality because it can deal with unconnected graphs. Betweenness centrality is a measure of the amount of influence that a node has over the flow of information in the graph. It is used to find the nodes that serve as bridges between different parts of the graph. Betweenness centrality of a node is computed as the number of shortest paths that pass through the node. Nodes that most frequently lie on these shortest paths have a higher betweenness centrality. PageRank[16] is the algorithm used by Google to rank web pages of search results. It is a measure of the transitive influence or connectivity of nodes that considers the number and the quality of the links to the node to determine its relevance. Relevant nodes are likely to receive a higher amount of links from other relevant nodes.

RESULTS

Analysis of Darknets

Table 1 presents the network metrics for i2p, Tor, and for the network that includes the nodes of both. To compute the metrics of this section, we created two subgraphs that included only the nodes in i2p and their connections, and only the nodes in Tor and their connections. We can see that the size of the networks differs significantly. Although Tor has many more nodes and edges, the differences for the average degree, average path length and diameter are not very large. As new domains join the network, they make a proportional number of new links and they remain close to the central nodes. Diameter is small, and density is low in all cases, which is common in networks that represent human activities.[17,18] Metrics of the graph that only contains the Tor nodes and of the graph that contains the nodes of both networks return similar values, except the number of connected components that is reduced significantly when the metric is computed for the complete graph. i2p nodes then increase the connectedness reducing the number of subgraphs (and of nodes) that are unreachable from the main component.

Figure 2 presents the graph including all Tor and i2p domains. The size of the nodes is proportional to the number of links (in-degree + out-degree). Only the nodes of the central connected component are included. Although there are many nodes and it is difficult to analyze specific nodes, we can still observe

TABLE 1. Metrics of the Networks (Graphs) that Included Only i2p Nodes, Only Tor Nodes, and All Nodes.

Metric	i2p (eepsites)	Tor (hidden services)	i2p + Tor (eepsites + hidden services)
Nodes	2687	46 562	49 249
Edges	13 857	282 270	304 673
Avg. degree	5.517	6.062	6.186
Density	0.002	<0.001	<0.001
Avg. path length	2.769	4.356	4.412
Diameter	8	11	12
Connected components	11	616	328

several patterns. Most i2p domains are clustered in the top left side forming a clear subnetwork. Several other i2p nodes are part of the "Tor side." Particularly, we can see two i2p hosting services (bottom left in the figure) that are primarily linked by Tor domains.

Metrics of the Domains

Nodes with the highest in-degree are listed in Table 2. In-degree accounts for the popularity of domains as measured by the number of services that link them. The first domain is incredibly popular, getting close to 50% of all the possible links. It is the DarkNet Light web that offers multiple Tor links. The out-degree of the second node is also very high since more than one-third of all possible services link it. It is a Tor hidden service onion crawler called FreshOnions (https://github.com/dirtyfilthy/freshonions-torscraper) that crawls the darknet looking for new hidden services and also finds hidden services from Clearnet sources. The remaining top five Tor domains are three Onion Lists of hidden services, like The Onion Crate (ranked 5), which offers a directory with thousands of classified websites from the dark web. The highest i2p node is ranked in position 12. It is followed by andmp.i2p, which is Daniel's Hosting, a free anonymous hosting service that can be found both in i2p and Tor. Since in-degree accounts for the number of services that link a given domain, it makes sense that most popular services are those that link and find other services.

Nodes with the highest out-degree are presented in Table 3. Out-degree measures the number of outgoing links of a given domain. The top domain is the i2p proxy service, which is followed by three different jump services from i2p (ranked 2–4). Since i2p jump services act as second layer proxies between client and host when the client does not have the address in its i2p "addressbook," it makes sense that these services are then the major hubs of the hidden networks providing links to more services than any other. Tor does not offer similar services and the findability of onions is limited mostly to lists. So results suggest that i2p proxy and jump services are an important entry point to the network. Daniel's hosting service from Tor is ranked fifth and it is the service with the highest out-degree of this darknet. The Tor mailbox service follows (ranked sixth). Still, the values of the out-degree for top-ranked nodes is much less when compared with in-degree. We can also observe that in-degree does not match out-degree in both rankings and also that the top-ranked services are different. In-degree and out-degree differ considerably for each node meaning that domains are either a provider of links or the subject of them. The low out-degree of the Tor services as compared to in-degree shows that this darknet is highly distributed when it comes to finding onions. The hubs of Tor are a hosting service and a mail service.

Top-ranked nodes in terms of closeness centrality (see Table 4) are Tor domains. The highest-ranked i2p node is in position 27, whereas the second i2p node is in position 967. Nodes with the highest in-degree also occupy top positions in terms of closeness centrality, suggesting that services massively pointed are in the central positions of the network being able to spread information efficiently. The top four domains are the same domains of the in-degree ranking. These include three Tor onion lists and the Tor hidden service onion crawler (FreshOnions). The Undernet Directory (UnderDir) completes the top 5. UnderDir is another onion list that classifies links by language and topic. The top-ranked i2p domain is Daniel's Hosting service. Closeness centrality is normalized, and the maximum possible value is 1. A value of 1 means that the node is connected to all other nodes by the minimum possible distance. Top-ranked nodes have very high values suggesting that they are very closely connected to all other nodes. So most of the nodes are directly linked to Onion lists or the FreshOnion crawler. Since these sites contain lists of services, results suggest that this information has a prominent and central position in the hidden networks.

Results of betweenness centrality are presented in Table 5. Top-ranked nodes include two domains from i2p and four domains from Tor. The node with the highest betweenness centrality is an i2p jump service "i2pjump.i2p." Rank second is the FreshOnions Tor service, which is the only top-ranked crawler. Daniel's Hosting Tor service ranks third in terms of betweenness centrality. Rank fourth is the DarkNet Light Tor website, and rank fifth is another onion list. In the sixth

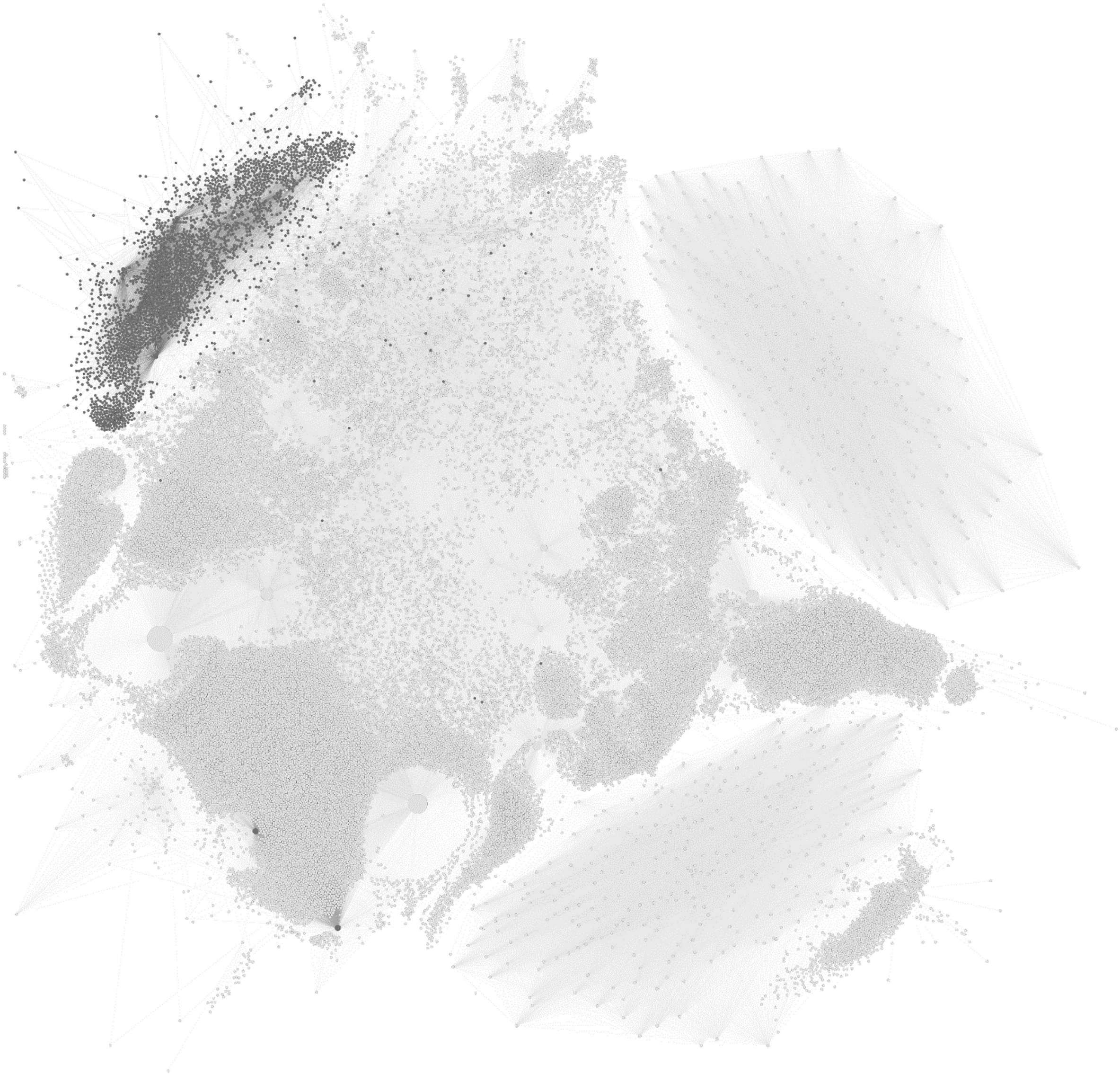

FIGURE 2. Graph of the central component of the Tor+i2p network. Light gray nodes represent Tor domains. Dark gray nodes represent i2p domains. Lines represent links. Size is proportional to the degree (in-degree+out-degree). The figure in high resolution is available at https://gitlab.com/ciberseg-uah/interconection-between-darknets-dataset.

TABLE 2. Nodes with the Highest In-Degree.

Rank	Domain	Network	In-Degree
1	pejjyyh7rhv5ctyu.onion	Tor	22 315
2	zlal32teyptf4tvi.onion	Tor	16 373
3	onionsnjajzkhm5g.onion	Tor	10 095
4	44llcbgyt22pwvyq.onion	Tor	6192
5	cratedvnn5z57xhl.onion	Tor	5332
...			
12	rv6zugykqdhmwwsuglv7j6...b32.i2p	i2p	3304
13	andmp.i2p	i2p	3211

position, we find the second i2p domain, "Hiddenanswers.i2p." Hiddenanswers is a question and answer website that is also present in Tor. The fact that domains from both networks are highly ranked reflects the importance of i2p domains as brokerage agents in the networks. The reduction of the number of connected components when both networks are analyzed together, previously mentioned, also supports this argument. The variety of services (jump service and Q&A from i2p, as well as crawler, hosting and onion lists from Tor) also suggest that all play a significant role in the darknet ecosystem. Betweenness centrality is a measure of the number

TABLE 3. Nodes with the Highest Out-Degree.

Rank	Domain	Network	Out-Degree
1	proxy.i2p	i2p	1793
2	stats.i2p	i2p	1205
3	no.i2p	i2p	1185
4	i2pjump.i2p	i2p	1177
5	dhosting4xxoydyaiv...syd.onion	Tor	535
6	Torbox3uiot6wchz.onion	Tor	337

TABLE 5. Nodes with the Highest Betweenness Centrality.

Rank	Domain	Network	Betweenness
1	i2pjump.i2p	i2p	43 755 077
2	zlal32teyptf4tvi.onion	Tor	41 176 352
3	dhosting4xxoydyaiv...syd.onion	Tor	32 290 935
4	pejjyyh7rhv5ctyu.onion	Tor	28 768 547
5	onionsnjajzkhm5g.onion	Tor	27 588 772
6	hiddenanswers.i2p	i2p	24 853 420

of shortest paths that go through a given node, and paths represent sequences of links that users follow in the darknets. So these particular nodes are in brokerage positions for the kind of service that they offer (jump, crawler, hosting, and onion list) in the paths that users follow and in the flows of information in the darknet.

Table 6 presents the nodes with the highest PageRank. Tor domains occupy top positions. The highest i2p domain is in position ten. PageRank measures the importance of a node in terms of the number and quality of the links to it. It returns the probability that a user randomly clicking on links will arrive to a site. Results show that Tor domains are more important than i2p domains. We can see that results are similar to other metrics as domains ranked in positions two (DarkNet Light), three (FreshOnions), and four (an onion list) are also highly ranked in terms of in-degree, closeness and betweenness. This suggests that the number of incoming links is also a good indicator of the position and influence of a domain. Ranked in the fifth position is another Tor onion list. However, when it comes to PageRank, the top domain is Daniel's Hosting, which also has a high in-degree (rank 17), out-degree (rank 5), and betweenness (rank 3). Since the PageRank score is substantially higher for the Tor hosting site, results suggest that this site is the most important domain and it will likely receive more visits than any other. DarkNet Light is the most important list of onion services in Tor, and it will likely receive many more visits than other onion lists that follow it in the ranking. identiguy.i2p is the top-ranked i2p domain (rank 10). It is an i2p jump service similar to the stats.i2p jump site.

TABLE 4. Nodes with the Highest Closeness Harmonic Centrality.

Rank	Domain	Network	Closeness
1	pejjyyh7rhv5ctyu.onion	Tor	0.706
2	zlal32teyptf4tvi.onion	Tor	0.642
3	onionsnjajzkhm5g.onion	Tor	0.580
4	44llcbgyt22pwvyq.onion	Tor	0.559
5	underdj5ziov3ic7.onion	Tor	0.513
...			
27	andmp.i2p	i2p	0.470

DISCUSSION

Results show that the most popular Tor websites are focused on indexing domains. Tor network does not have a public index with all the hidden domains, so several websites just maintain lists of popular and new domains. Hence, to further index and study the hidden services in Tor, we should focus first on the top-ranked domains for the different metrics. These are the most critical sites to start mapping the darknets.

As for i2p, the most important domains are jump and proxy sites. Due to the way i2p works, normally, these sites are the most relevant. To access eepsites, it is necessary to use a jump site. Jump sites act as a DNS service to access i2p domains. Hence, if we want to index and study i2p network, the eepsites that are top-ranked in out-degree and betweenness centrality should guide the investigation.

Results also show that other types of sites have prominent positions in each darknet. In Tor, one of the services with the highest out-degree is TorBox mail service, suggesting that this Tor service is used mostly to point to other hidden services. This may be an indicator of the fact that a lot of illegal activities use TorBox as an e-mail server.[19–21] As for i2p, results for betweenness

TABLE 6. Nodes with the Highest Pagerank Centrality.

Rank	Domain	Network	PageRank
1	dhosting4xxoydyaiv...syd.onion	Tor	3492
2	pejjyyh7rhv5ctyu.onion	Tor	2897
3	zlal32teyptf4tvisyd.onion	Tor	1478
4	onionsnjajzkhm5g.onion	Tor	1129
5	donionsixbjtiohce2...ead.onion	Tor	1077
...			
10	identiguy.i2p	i2p	778

centrality suggest that *hiddenanswers.i2p* plays a significant role in the communication paths of the network. Hiddenanswers is a site with similar functionality to Yahoo Answers (https://answers.yahoo.com/) but without any kind of censorship. Hiddenanswers is also present in Tor. The duplicity of this as well as other services further strengthens the assumption of the interconnection and the dual nature of the communication between Tor and i2p.

Previous research focuses on describing or improving the security of Tor.[3,4] Several datasets of Tor have been reported and analyzed, like DUTA-10K [11]. We compared our dataset with it, showing that our approach provides a broader coverage of Tor. Further, our work also recorded i2p eepsites, reporting the connections between Tor and i2p. To the best of our knowledge, there are no datasets or studies that systematically map i2p structure. Research on i2p focuses on monitoring and attacking i2p users [22,23]. Our results provide a map of both darknets and their connections, which is used to find the most relevant sites in terms of different network metrics. The dataset is publicly accessible in GitLab at https://gitlab.com/ciberseg-uah/interconection-between-darknets-dataset.

SCENARIOS OF USE FOR LEAS

The dataset and findings presented in this article can help LEAs to investigate darknet illegal activities in different ways. First of all, this article evidences the existence of cross operations between i2p and Tor, stressing the necessity to investigate i2p discover Tor domains. Past operations of LEAs mostly focused on Tor, [24,25] and because of this, cybercriminals are probably moving to i2p. LEAs need to be aware of this and focus on other darknets, since they offer different and complementary services. LEAs can also use the dataset to investigate current Tor and i2p domains. They can find existing domains and track their connections. They can also run new analyses to investigate the positioning and influence of services. Furthermore, our analysis of the dataset provides a list of current key sites of Tor and i2p. LEAs can use it as a starting point to crawl and monitor the darknets using the methods presented in the section titled “Dataset Creation.” LEAs could then create new mappings that include services potentially leading to new criminal activity. Knowing the main types of services in the darknet ecosystem could guide future investigations. This is particularly important because darknet services are highly volatile. Even if a given domain goes offline, it is likely that it will be replaced by other offering similar functionalities. As hidden services can appear and disappear relatively quickly, crawling the darknet at a given moment provides a snapshot that LEAs can use to monitor suspicious activity. These can be improved in the future to create dynamic views of the Darknet or of a part of it, which may even raise alerts when given events happen. For instance, when a service comes online.

Another possible scenario in which the dataset can be useful is when LEAs try to take down criminal sites. This often involves performing some kind of cyberattack over them, which usually is the only option due to the built-in opacity of darknets. Discovering as much as possible of the attack surface of an objective is crucial to find weaknesses that can be used to define attack vectors. The dataset can help to find services that are present in Tor and i2p. There is the possibility that a service can be securely deployed in Tor but not in i2p or the other way around. LEAs can try to attack the i2p exposed service to take down or take control of the site.[26] (Alphabay and Hansa darknet markets shut down after international police operation. https://www.dw.com/en/alphabay-and-hansa-darknet-markets-shut-down-after-international-police-operation/a-39776885). Our analysis of the dataset already pointed to prominent sites that are mirrored in Tor and i2p (like hosting services) showing how they can be found. It also suggests the necessity of finding all the access points of criminal services in the Darknet to expose their complete attack surface and bring them down for good. LEAs can also analyze the current dataset to find other services that may be mirrored.

CONCLUSION

This article presents the results of analyzing a dataset with data of i2p and Tor networks. We also report the process of creating the dataset. To the best of our knowledge, this is the only dataset that connects eepsites and hidden services.

Using graph analysis, we showed that crawling one darknet can improve the discovery of sites present on a different darknet. Also, this study helps to understand the positioning of sites and their influence in the network.

Graph metrics return similar values for most measures suggesting that both darknets are structurally similar. The reduction of the number of connected components, when all nodes are included in a single graph, suggests that i2p nodes play an important role in making more Tor nodes reachable.

Node metrics suggest that in terms of centrality, Tor onion lists and the Tor FreshOnions crawler occupy central positions and get most of the links playing a substantial role in the spreading information.

i2p jump services are the main hubs of the network (top-ranked out-degree) pointing to many other nodes. Results of betweenness centrality suggest that all main darkenet services (jump, crawl, hosting, and onion lists) play an important role in the communication paths of the darknets. The most significant actors for each role are i2pjump.i2p, the FreshOnions Tor crawler, Daniel's Tor hosting, and the DarkNet Light Tor website (onion list).

The most important Tor domains are hosting and index websites. Furthermore, the most important i2p domains are jump sites. Since Tor does not offer effective search engines, index websites partially address this limitation. So i2p jump sites become the relevant hubs of the darknet.

REFERENCES

1. M. Chertoff and T. Simon, "The impact of the dark web on internet governance and cyber security," Feb. 2015. [Online]. Available: https://www.cigionline.org/publications/impact-dark-web-internet-governance-and-cyber-security
2. G. Owen and N. Savage, "The Tor Dark Net," Centre for International Governance Innovation and the Royal Institute of International Affairs, Sep. 2015. [Online]. Available: https://www.cigionline.org/publications/tor-dark-net
3. R. Snader and N. Borisov, "A tune-up for Tor: Improving security and performance in the Tor network," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2008, vol. 8, p. 127.
4. D. McCoy, K. Bauer, D. Grunwald, T. Kohno, and D. Sicker, "Shining light in dark places: Understanding the Tor network," in *Proc. Int. Symp. Privacy Enhancing Technol. Symp.*, 2008, pp. 63–76.
5. K. Loesing, S. J. Murdoch, and R. Dingledine, "A case study on measuring statistical data in the Tor anonymity network," in *Proc. Int. Conf. Financial Cryptography Data Secur.*, 2010, pp. 203–215.
6. D. S. Dolliver, "Evaluating drug trafficking on the Tor network: Silk road 2, the sequel," *Int. J. Drug Policy*, vol. 26, no. 11, pp. 1113–1123, 2015.
7. M. Wilson and B. Bazli, "Forensic analysis of I2P activities," in *Proc. IEEE 22nd Int. Conf. Autom. Comput.*, 2016, pp. 529–534.
8. B. Bazli, M. Wilson, and W. Hurst, "The dark side of I2P, a forensic analysis case study," *Syst. Sci. Control Eng.*, vol. 5, no. 1, pp. 278–286, 2017.
9. E. Nunes *et al.*, "Darknet and deepnet mining for proactive cybersecurity threat intelligence," in *Proc. IEEE Conf. Intell. Secur. Inform.*, 2016, pp. 7–12.
10. A. Chaabane, P. Manils, and M. A. Kaafar, "Digging into anonymous traffic: A deep analysis of the Tor anonymizing network," in *Proc. IEEE 4th Int. Conf. Netw. Syst. Secur.*, 2010, pp. 167–174.
11. M. W. Al-Nabki, E. Fidalgo, E. Alegre, and L. Fernández-Robles, "Torank: Identifying the most influential suspicious domains in the Tor network," *Expert Syst. Appl.*, vol. 123, pp. 212–226, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0957417419300296
12. C. Iliou, G. Kalpakis, T. Tsikrika, S. Vrochidis, and I. Kompatsiaris, "Hybrid focused crawling for homemade explosives discovery on surface and dark web," in *Proc. IEEE 11th Int. Conf. Availability, Rel. Secur.*, 2016, pp. 229–234.
13. S. M. Goodreau, "Advances in exponential random graph (p*) models applied to a large social network," *Social Netw.*, vol. 29, no. 2, pp. 231–248, 2007.
14. I. Sanchez-Rola, D. Balzarotti, and I. Santos, "The onions have eyes: A comprehensive structure and privacy analysis of Tor hidden services," in *Proc. 26th Int. Conf. World Wide Web*, 2017, pp. 1251–1260.
15. G. Noubir and A. Sanatinia, "Honey onions: Exposing snooping Tor HSDir relays," in *Proc. DEF CON 24*, 2016.
16. S. Brin and L. Page, "The anatomy of a large-scale hypertextual web search engine," *Comput. Netw. ISDN Syst.*, vol. 30, no. 1–7, pp. 107–117, 1998.
17. D. Chakrabarti and C. Faloutsos, "Graph mining: Laws, generators, and algorithms," *ACM Comput. Surv.*, vol. 38, no. 1, p. 2, 2006.
18. A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee, "Measurement and analysis of online social networks," in *Proc. 7th ACM SIGCOMM Conf. Internet Meas.*, 2007, pp. 29–42.
19. R. B. Yetter, "Darknets, cybercrime & the onion router: Anonymity & security in cyberspace," Ph.D. dissertation, Utica College, Utica, NY, USA, 2015.
20. D. S. Dolliver, "Emerging technologies, law enforcement responses, and national security," *I/S: J. Law Policy Inf. Soc.*, vol. 15, p. 123, 2019.
21. W. F. Gross Jr, "Monitoring and tracking ISIS on the dark web," in *Online Terrorist Propaganda, Recruitment, and Radicalization*. New York, NY, USA: Taylor & Francis, 2019, p. 341.
22. C. Egger, J. Schlumberger, C. Kruegel, and G. Vigna, "Practical attacks against the I2P network," in *Proc. Int. Workshop Recent Adv. Intrusion Detection.*, 2013, pp. 432–451.
23. J. P. Timpanaro, C. Isabelle, and F. Olivier, "Monitoring the I2P network," 2011. [Online]. Available: https://hal.inria.fr/hal-00653136/document

24. "Double blow to dark web marketplaces." [Online]. Available: https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces
25. W. Lacson and B. Jones, "The 21st century darknet market: Lessons from the fall of silk road," *Int. J. Cyber Criminol.*, vol. 10, no. 1, pp. 40–61, 2016.
26. R. van Wegberg and T. Verburgh, "Lost in the dream? Measuring the effects of Operation Bayonet on vendors migrating to dream market," in *Proc. Evol. Darknet Workshop*, 2018, pp. 1–5.

CARLOS CILLERUELO is currently a Researcher with the University of Alcalá, Alcalá de Henares, Spain (2018–present), where he has also been working toward the Ph.D. degree since 2018. Previously, he was with several companies as a cybersecurity and forensics specialist. He also participated in an Erasmus+ program on data forensics (2013). He is a research member of the ProTego EU H2020 project focused in cybersecurity and e-health (2019–2021). He presented the results of his work at the RootedCon-2020 Conference. His current research focuses on cybersecurity, particularly in the areas of forensics, darknets, and machine learning applied to cybersecurity. He received the B.Sc. degree in computer science in 2015 and the M.Sc. degree in cyber security in 2016. He is the corresponding author of this article. Contact him at carlos.cilleruelo@uah.es.

LUIS DE-MARCOS has been an Associate Professor with the University of Alcalá, Alcalá de Henares, Spain, since 2015. He is a Principal Investigator of the Research Team of the ProTego Project (H2020) on Cybersecurity (2019–2021), and was a Principal Investigator in two national research projects in Spain (2011–2013). He was a Research Fellow with Lund University, Lund, Sweden, in 2007 and 2009, the University of Reading, Reading, U.K., in 2008, the Monterrey Institute of Technology, Monterrey, Mexico, in 2010, and the University of Zagreb, Zagreb, Croatia, in 2018. He has more than 100 refereed publications in conferences and journals. His research interests include educational technologies, e-learning, and cybersecurity. He received the B.Sc. and M.Sc. degrees in computer science in 2001 and 2005, respectively, and Ph.D. degree in information, documentation, and knowledge in 2009. Contact him at luis.demarcos@uah.es.

JAVIER JUNQUERA-SÁNCHEZ is a Researcher with the University of Alcalá, Alcalá de Henares, Spain (2018–present), where has also been working toward the Ph.D. degree since 2020. Previously, he was with several companies as cybersecurity analysts and software developer. He is a research member of the ProTego EU H2020 project focused in cybersecurity and e-health (2019–2021). He presented the results of his work at the RootedCon-2020 Conference. His research interests include cybersecurity, software security, cryptography, and darknets. He received the B.Sc. degree in computer science in 2018 and M.Sc. degree in cyber security in 2019. Contact him at javier.junquera@uah.es.

JOSE-JAVIER MARTÍNEZ-HERRÁIZ has been an Associate Professor with the Department of Computer Science (Artificial Intelligence Area), University of Alcalá, Alcalá de Henares, Spain (since 1994), where he is the Rector's Delegate for Electronic Administration and Security. He was with private telecommunication business companies (Spain and Italy) as a Software Analyst, Project Manager, and Consultant between 1988 and 1999. He was the Director of the Computer Science Department between 2008 and 2011. He has collaborated extensively with Spanish law enforcement agencies and cybersecurity companies, and his work was awarded with Order of Merit of the Police Forces (2011 and 2015). He has practical experience in software development, technology and modeling, methodologies for software projects, planning and management, software maintenance, e-learning, gamification technology, and cybersecurity. He received the degree in computer science from the Polytechnic University of Madrid, Madrid, Spain, and the Ph.D. degree from the University of Alcalá in 2004. Contact him at josej.martinez@uah.es.

3.3 Summary of the results of Article 2

This chapter has presented an analysis of the interconnection between Tor and i2p darknets. The search for stolen medical information led to this discovery. This research have detected how some users combine the usage of multiple privacy technologies to exchange information. Moreover, the usage of graph analysis techniques allows the identification of the most important services offered in those networks. The graph analysis presented is extremely useful in analysing darknet data, and can be used for identifying the most popular or influential sites. For example, a LEA can use graph analysis to determine and detect the most popular dark markets, and thus prioritise its closure over others. Furthermore, this investigation has released the first public i2p and Tor dataset, currently available at Gitlab. This dataset fulfils several purposes and utilities. On one hand, allow the recreation and further analysis of the graphs presented on the paper. On the other hand, can be used as a init URL dataset for the development of a crawler. Any crawler needs some introduction URL point to start its indexing process, and this dataset can provide multiple introduction points to feed a crawler.

In summary, this research proves the benefits of combining information from several darknets. If we do not obtain data from the i2p network we will be missing relevant information from Tor and vice-versa. As a consequence of this study, the analysis of darknets makes it possible to identify the actors and information involved in criminal activities [88][8], as well as proving the benefits of using Graph Analysis techniques to explore and identify important sites on those networks. Furthermore, the recent rise of Ransomware as a Business (RaaB) models have led to the attack of numerous healthcare infrastructures and services, and all those criminal groups use Tor as a method of communication and extortion [16][17].

After this research, only the final research objective of this thesis needed to be addressed, The study of the cybersecurity status of modern IoT medical devices. Medical information is stored in common or adapted technologies such as databases but in the end, these technologies have some point in common or are accessible through computers. On the other hand, IoT devices present custom implementations of hardware and protocols, and in the case of medical IoT devices can be in charge of diagnosis or treatments. Reducing or eliminating its failure tolerance. So in order to research this field I decided, with the limited means and budgets available at my disposal, to buy and audit an IoT medical device. In the next chapter, a detailed security analysis of IoT medical devices and their results will be presented.

Chapter 4

Healthcare device security

4.1 Paper 3 contribution

Besides traditional software and computers Healthcare, like any other industry, has involved and developed specific technological devices. Right now, most of the diagnosis and treatment devices running in Hospitals have some kind of embedded operative system and proprietary software, that is usually concealed and only known by the manufacturer. Those devices, unfortunately, usually have not been properly tested on cybersecurity.

Right now, there is a lack of regulation in this aspect and most manufacturers have been focused on safety, and not cybersecurity. Devices are designed and tested to not affect the health of the patient and to guarantee their safety. The diagnosis or treatments are carefully controlled to not affect any patient and seen in the past with incidents such as Therac-25 software bugs [89], but cybersecurity is usually left out of these tests and considerations. Being this the current situation, where the majority of manufacturers do not check or comply with cybersecurity needs, multiples cybersecurity vulnerabilities has been discovered through the years in multiple medical devices [90][53][91].

In order to prove some of the premises, this chapter presents an independent analysis of an IoT medical device, Kardia Mobile [14], currently in use by several Hospitals. This device is a small IoT electrocardiograph that enables the easy creation of electrocardiograms by patients. Using this device is possible to perform patient monitoring and successfully replace some visits to Hospital centres. The following paper also uses a methodology that can be applied in the auditing of medical devices and the detailed audited process of the device. Moreover, this paper presents the discovery of several cybersecurity vulnerabilities, that are also carefully explained and published.

4.2 Paper 3

The third scientific paper is included below, “Security and privacy issues of data-over-sound technologies used in IoT healthcare devices”.

2021 IEEE Globecom Workshops (GC Wkshps) | 978-1-6654-2390-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/GCWkshps52748.2021.9682007

Security and privacy issues of data-over-sound technologies used in IoT healthcare devices

Carlos Cilleruelo
Computer Science Department
Universdad de Alcalá
Alcalá de Henares, Spain
carlos.cilleruelo@uah.es

Javier Junquera-Sánchez
Computer Science Department
Universdad de Alcalá
Alcalá de Henares, Spain
javier.junquera@uah.es

Luis de-Marcos
Computer Science Department
Universdad de Alcalá
Alcalá de Henares, Spain
luis.demarcos@uah.es

Nicolas Logghe
Computer Science Department
Universdad de Alcalá
Alcalá de Henares, Spain
nicolas.logghe@edu.uah.es

Jose-Javier Martinez-Herraiz
Computer Science Department
Universdad de Alcalá
Alcalá de Henares, Spain
josej.martinez@uah.es

Abstract—**Internet of things (IoT) healthcare devices, like other IoT devices, typically use proprietary protocol communications. Usually, these proprietary protocols are not audited and may present security flaws. Further, new proprietary protocols are desgined in the field of IoT devices, like data-over-sound communications. Data-over-sound is a new method of communication based on audio with increasing popularity due to its low hardware requirements. Only a speaker and a microphone are needed instead of the specific antennas required by Bluetooth or Wi-Fi protocols. In this paper, we analyze, audit and reverse engineer a modern IoT healthcare device used for performing electrocardiograms (ECG). The audited device is currently used in multiple hospitals and allows remote health monitoring of a patient with heart disease. For this auditing, we follow a black-box reverse-engineering approach and used STRIDE threat analysis methodology to assess all possible attacks. Following this methodology, we successfully reverse the proprietary data-over-sound protocol used by the IoT healthcare device and subsequently identified several vulnerabilities associated with the device. These vulnerabilities were analyzed through several experiments to classify and test them. We were able to successfully manipulate ECG results and fake heart illnesses. Furthermore, all attacks identified do not need any patient interaction, being this a transparent process which is difficult to detect. Finally, we suggest several short-term solutions, centred in the device isolation, as well as long-term solutions, centred in involved encryption capabilities.**

Index Terms—**Communication system security, Data security, Internet of Things, Health devices**

I. Introduction

Nowadays multiple IoT healthcare devices are being used by hospital staff and patients. Over the years, Implantable Medical Devices (IMDs) and Implantable Cardiac Defibrillators (ICDs) have been adding wireless communication capabilities. But other IoT healthcare device has also been improving their interconnectivity and wireless communications technologies, like insulin pumps or mobile electrocardiographs. The patients can carry these small electrocardiographs where they can perform periodic electrocardiograms (ECGs) that will be sent to their corresponding medical specialist. These novel IoT devices facilitate monitoring and earlier diagnosis of patients, avoiding numerous hospital visits. Similar to other devices in the IoT industry, some of these devices are using proprietary protocols or involve new methods of communications. One of these new emerging communications technologies used for healthcare devices is known as data-over-sound.

Data-over-sound presents an alternative to traditional radio frequency (RF) communications granting several advantages over RF. Data-over-sound avoids the necessity of using specific hardware since just a microphone and speaker are needed to establish the communications. This also has the advantage of bypassing other problems like radio frequency interference. As mentioned these advantages bring several benefits, but the cybersecurity of novel protocols and implementations need to be evaluated. Data-over-sound protocols are a low-cost solution in comparison with Wi-Fi or Bluetooth protocols, but due to its novelty, this technology has been less audited and tested in applications, like IoT healthcare devices where sensitive data is being transmitted. It is also necessary to take into account, that even though attacks against external IoT devices like mobile electrocardiographs do not represent the same risk as IMDs or ICDs devices, they still manage healthcare information which is taken into account for medical decisions.

This paper presents an analysis of an IoT healthcare device, a mobile electrocardiograph, which is capable of maintaining data-over-sound communication with a smartphone. We performed reverse engineering analysis of this IoT healthcare device and its data-over-sound protocol, following a black-box approach. This process allowed us to analyze the data-over-sound proprietary protocol used in this IoT healthcare device and discover several cybersecurity vulnerabilities.

In summary, we make the following contributions:

- We reverse engineer and analyse an IoT healthcare device capable of performing wireless data-over-sound commu-

978-1-6654-2390-8/21/$31.00 ©2021 IEEE

nications.

- We identified several cybersecurity vulnerabilities in this specific device due to the nature of the data-over-sound protocol used and its implementation.
- We present short-term and long-term solutions in order to address and mitigate the discovered vulnerabilities.

Besides these contributions, all vulnerabilities and problems presented in this paper followed a responsible disclosure process. The manufacturer and the Cybersecurity and Infrastructure Security Agency (CISA) were notified, prior to publication and submission of this paper. And as an additional step, all references to the specific product and manufacturer have been omitted from this paper, since the manufacturer is still working on possible mitigation solutions.

The remainder of this paper is structured as follows. Section II presents an overview of the related work, a general view of the security status in healthcare devices, and information about data-over-sound technology protocols used in the industry and their evolution. Section III describes the methodology for the analysis of the device and the laboratory setup used for experimentation. Section IV shows the processes taken for reverse-engineering the data-over-sound protocol and presents the weaknesses found. Section V presents the different cybersecurity vulnerabilities and attacks discovered. Section VI analyzes the attacks and proposes short-term and long-term solutions. Finally, Section VII provides concluding remarks.

II. Related work

Cybersecurity problems in healthcare devices are not something new. Several papers and researches have explored the lack of cybersecurity measures in technological healthcare devices [1]. Usually, these researches have been focused on Implantable Medical Devices (IMDs), like pacemakers [2] or Implantable Cardiac Defibrillators (ICDs) [3]. The evolution of medical devices into connected devices or healthcare IoT has provoked the discoveries of numerous vulnerabilities [4]. The use of Radio Frequency Identification (RFID), Wi-Fi or other proprietary radio protocols [3] are normally part in IoT healthcare devices without implementing proper cybersecurity measures.

Many possible solutions to these attacks have been presented in recent years. Several propositions involve the use of external devices acting like proxies [5] [6] to protect the communications on healthcare devices. Although the use of proxies mitigates some attacks, it has been demonstrated incapable of offering a full security solution, being affected by Man-In-The-Middle (MITM) attacks [7] or eavesdropping using MIMO-based attacks [8]. On the other hand, other research papers involve the use of cryptography algorithms to protect healthcare device communications [9]. However, the use of cryptography usually implies the need for more computational power on devices or dedicated hardware. This directly affects the manufacturing cost and energy consumption of IoT devices.

Nevertheless, even though there are numerous researches around different healthcare devices and how to implement cybersecurity measures on these devices, the lack of actual regulations and standards around IoT security or medical device security results in the discovery of serious vulnerabilities. There are some U.S regulations like Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act, centred in healthcare data regulation but they usually do not present any clear indications on how to protect private information or cybersecurity measures to be taken into account. This establishes the necessity of new cybersecurity industry standards like the proposed by Strielkina et al. [10]. These standards should be included in mandatory healthcare regulations, independent of novel technological solutions, forcing new IoT healthcare devices to be cybersecurity compliant.

A. *Data-over-sound communications*

As previously mentioned the device studied in this article uses data-over-sound communications. Due to the usage of this novel type of communication, it is necessary to review and explain the status of data-over-sound communications, also known as Audio Data Transmission (ADT). Data-over-sound presents an alternative to traditional radio frequency communications and has been successfully used in several scenarios. Zhang et al. successfully develop an emergency warning system using digital audio broadcast [11]. And independently of research projects, several companies are developing data-over-sound communication protocols [12]. Additionally to the previously mentioned works, several open source projects that implement data-over-sound libraries can be found on GitHub [13] [14].

III. Methodology

A. *Thread modeling - STRIDE*

Before performing any test over the IoT healthcare device, we built a threat model based on STRIDE framework [15]. This framework provides a mnemonic for security threats, classified in six categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of privilege. These threats face Authentication, Integrity, Non-repudiation, Confidentiality, Availability and Authorization; respectively. STRIDE is used because it also offers a systematic manner to develop the analysis. Even though our research is focused on data-over-sound communications, obtaining the complete landscape of the system allowed us to detect and assess the impact of a vulnerability in the ECG recording process. Figure 1 shows a Data Flow Diagram (DFD, also known as Threat Modelling Diagrams [16]), of an IoT healthcare device and its communications. This DFD allows us to obtain a software-centric vision of the architecture from where we can characterize the threats.

The DFD, along with the STRIDE categorization, allows both narrowing the attack surface exposed to each threat, as well as measuring the risk it contributes to the entire system. Thus, we can deduce the scope affected by a threat acting over the HR Audio flow.

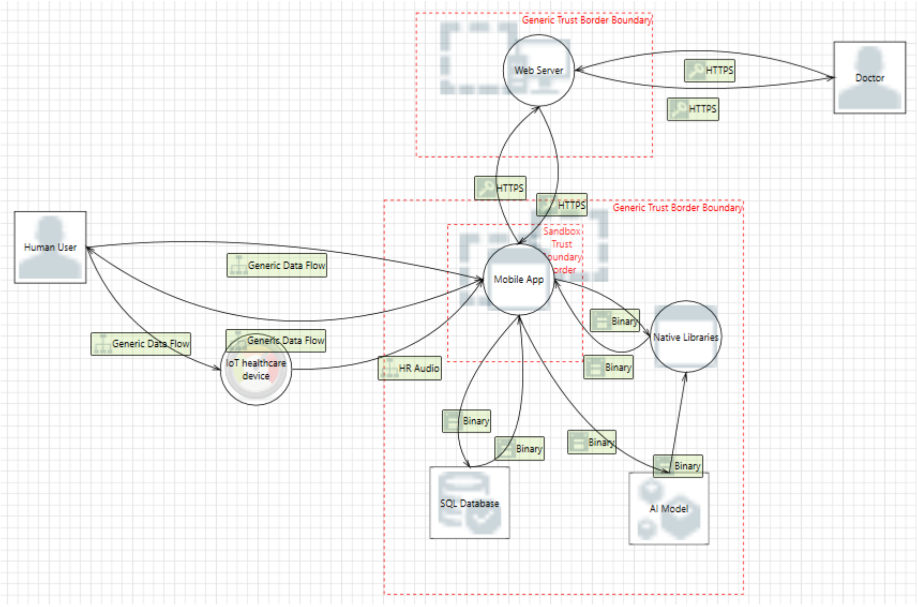

Fig. 1. Data Flow Diagram

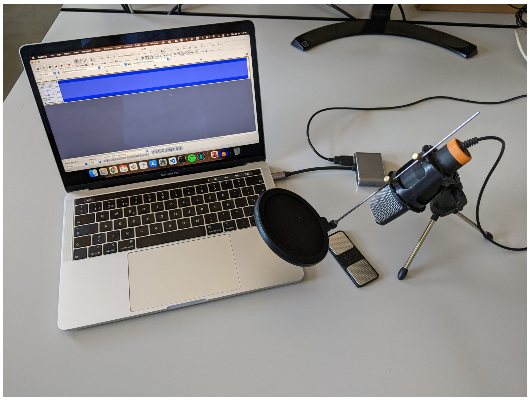

Fig. 2. Laboratory setup

B. Laboratory setup

Figure 2 shows our laboratory setup, composed of a laptop, the IoT healthcare device and the external microphone. More sophisticated equipment like a directional microphone could also be used to extend the range of possible attacks. But taking into account, that all the device communications are performed via sound, any device with a microphone and speakers could be used as a transceiver. As support tools, several software audio solutions have been used in the analysis and experiments, like Audacity [17] and Sonic Visualiser [18]. Audacity allowed us to capture and modify data-over-sound communications, and Sonic Visualizer allows us to perform different visualisations of these communications. Also, it is necessary to mention that all the analyses have followed a black-box reverse-engineering approach.

IV. Reverse-engineering data-over-sound communications

First of all, we studied the possibilities of communication of the IoT device. After analyzing the mobile application, we realized that the IoT healthcare device was sending information through audio. The mobile application requested microphone permissions and asks for the deactivation of mobile NFC communications. However, we were unable to listen to anything so we decided to make some recordings using a microphone. Initially, the recording suggested that the transmission was being done in a very low volume: the manufacturer instructions state that the device must be near the phone, and there was just a faint waves in the wave plot generated by Audacity.

Later on we proceeded to take other recordings, using Audacity, while the IoT healthcare device was producing an ECG. After analyzing the audio recordings with a spectrogram (see Figure 3)), we realized there was data in the high frequency band of the spectrum. Hence, we are facing some kind of data-over-sound protocol. This analysis also showed that the IoT device uses ultrasounds to perform the transmission and communications.

A. Data-over-sound characterization

Anything over $10kHz$ is pretty much inaudible and also used in many other applications since most everyday sounds (included other sound-based control systems, like phone signalling [19]) occur at frequencies below $4kHz$. This situation, makes higher frequencies a perfect medium for transmitting data. Sounds somewhat below $20kHz$, which are also inaudible to a human listener, are still considered to be in the ultrasonic range and can be captured by common microphones.

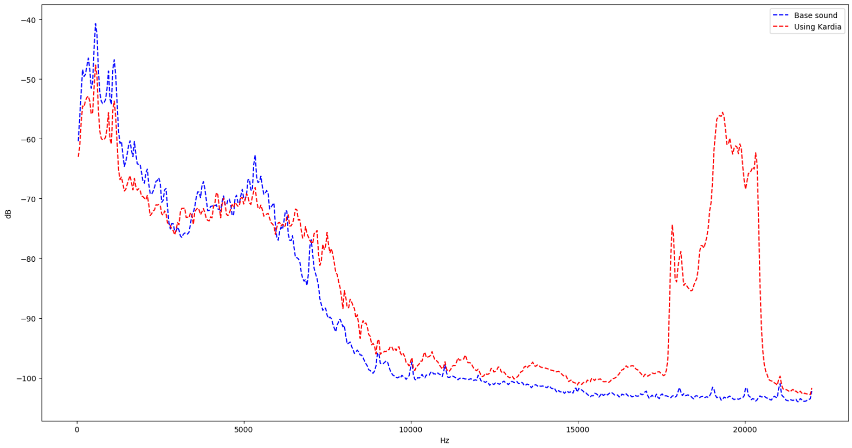

Fig. 3. Spectrogram of the IoT device audio

This provides a limited frequency band that can be used for data transmission.

Subsequently, we performed a waterfall analysis, showing that the frequency oscillates over time around $19.200KHz$. Due to the oscillation range, the chart also suggests the data values could be modulated over frequency (i.e, Frequency Modulation, or FM). In FM, the values are modulated in the wave increasing or decreasing its frequency (for encoding up and low values, respectively).

To evaluate how the ECG signal was transmitted, we developed a fuzzing script. The experiment proceeded as follows:

1) Create the message to transmit: As the ECG mobile application draws the ECG in live-time, our script generates a sinus function as a baseband signal, to check how it interferes with the cardiogram drawing. To emulate a heartbeat of 60bpm, we discretized the sinus, obtaining 44100 values of one period (i.e., a 44100 values audio sampling). It transforms the sinus formula into an array with values between -1 and 1.
2) Modulate the message in FM: Here, we also used a sinusoidal carrier to generate a reproducible WAV file. We calculated the discrete values that the signal should have, using the sinus formula. Using the values of the message, we applied them to vary the frequency of the signal. As the WAV file is also discrete (i.e., also has a sampling rate, set in 44100 samples per second), we applied the formulas from the Equation 1 to obtain each sample i. Where t is the time of the period where the sample has to be calculated; f_i is the frequency of the signal in base to the message value m_i, and $sample_i$ is the value of the signal for the sample i.

$$t = (i \mod 44100)/44100 \tag{1}$$

$$f_i = 19200 + 1000 * m_i \tag{2}$$

$$sample_i = \sin 2 * \Pi * f_i * t \tag{3}$$

3) Observe the results in the mobile application

After analyzing for the first time the figure drawn in the application, following the playing of the WAV file, the image resulted in the representation of a sinus wave. This information allowed us to conclude that the IoT device did not perform any additional protection to the ECG signal, besides modulated it into frequency domain.

V. Results

The previously reverse engineering analysis of the communication protocols of the device allows us to discover several cybersecurity vulnerabilities. These vulnerabilities resulted in several types of active and passive attacks which are presented following the STRIDE methodology.

A. *Spoofing*

Our analysis of the proprietary data-over-sound protocol demonstrated the lack of encryption and authentication in the communication process between the IoT device and a smartphone. This lack of encryption in the communication directly leads to the possibility of performing spoofing attacks.

This makes possible the generation of fake signals and altering ECG values based on the objectives of an attacker. For example, as shown in Figure 4 it is possible to generate a signal that will generate a fake ECG, as shown in Figure 4. Using this same technique is also possible to generate ECG classified as tachycardia and other heart issues.

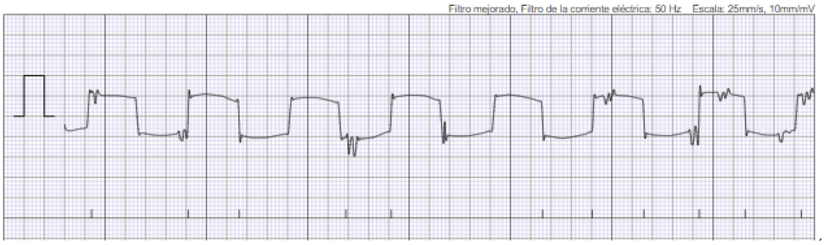

Fig. 4. Fake ECG generated through custom data-over-sound

B. *Tampering*

This lack of encryption and authentication could also turn into a more sophisticated scenario like tampering. Whenever a patient is using the device, an evil twin attack can be done. In the event that the user is going to take a measurement, it is possible to simultaneously generate a stronger signal, that will affect the results of the ECG.

We were able to impersonate the genuine device and tamper an active ECG session from a distance of $25m$ just using a laptop. An attacker with a directional speaker, or with a louder one, could be able to perform this attack from a larger distance.

C. *Repudiation*

The easiest of these attacks can be a replay attack, where an attacker is able to capture a wireless communication and later replay it against the device. The device lacks any type of repudiation technology, any data-over-sound captured can be replayed at any time and its transmission will always be accepted.

D. *Information disclosure*

Following the lack of encryption and authentication, an attacker can be centred on stealing private information. The messages exchanged between the devices did not seem to include patient data, like names or usernames, but it is possible to recover the ECG data sent from other devices. Passive adversaries can compromise the patient's privacy just by eavesdropping on the wireless sound channel while there is ongoing communication. On the other hand, this attack is limited due to the fact that the attacker has to be near the target patient. But it is also needed to take into account that adversaries could use sophisticated equipment, like a directional microphone to extend the distance from which they can perform these attacks. However, being this a passive attack, the attacker would need to wait until the device exchanges data to complete a successful eavesdropping attack.

E. *Denial-of-Service*

The lack of security measurements in the data data-over-sound protocol used in the IoT healthcare device also results in Denial-of-Service (DoS) vulnerabilities. An attacker can easily perform a DoS attack by continuously sending noise in frequencies near $20kHz$. Therefore, jamming the genuine sound generated by the IoT healthcare device is possible by playing alternative sounds at a higher volume, as will still be inaudible by humans.

VI. Discussion

First of all is it necessary to take into account that the severity of these attacks are limited due to the necessity of being in a relatively short distance between the attacker and the objective, around 25 meters. After taking this into account, the device lacks of any minimal security measures and the severity of this attacks could be classified as medium just because of the previously mentioned context. Furthermore, all the presented attacks were further tested to determine how easy it could be to tamper the signal without any special hardware devices (e.g., just with a computer, or a smartphone).

A. *Short-term solutions*

Short-term measures that can be applied to resolve the mentioned issues could be the use of the IoT healthcare device in an isolated and close environment. If we do not have anyone near our ECG measurement and we are in a close environment, we make it practically impossible to be able to perform the previously mentioned attacks. This is a possible short-term and easy solution. Another recommendation is to bring the device as close as possible to the smartphone. If the IoT device is closer to the microphone smartphone than the attacker, it will make more difficult some attacks, like replay or tampering. Because the strength of our data-over-sound signal will be greater than the attacker.

B. *Long-term solutions*

The use of properly authenticated and encrypted channels can be a possible countermeasure to the proposed attacks. The usage of data-over-sound communications does not imply that encryption and authentication can not be applied. For example, previously mentioned commercial solutions like Sonarax [12] uses encryption for its implementation. The problem of the analysed IoT device is not the usage of data-over-sound communications but its implementation.

Even though a device can only transmit data (i.e., it has no input capabilities), it could have some type of identification. This identification could allow the user to pre-register the IoT device before establishing communications. This identification could be encoded as a QR code signed by the manufacturer, or use any type of signed beacon [20]. Moreover, this spoofing mitigation will also prevent possible replay attacks [21].

But with a pre-registered device, the transmissions could be authenticated using any type of TAN code, as proposed by Starnberger et al. [22]. This protection could also allow the mitigation of tampering attacks.

On the other hand, denial of service attacks present a difficult challenge. Even though there exist some approaches against jamming in other transmission channels (like channel-hopping in RF [23]), the data-over-sound technologies are not very reliable in that aspect [24].

VII. Conclusion

In this work we analyzed the security and privacy of an IoT healthcare device capable of perform data-over-sound communications. To accomplish this objective we acquired a novel and small IoT device capable of perform ECGs. This device was analyzed following the STRIDE thread modeling methodology, and as a result several vulnerabilities were identified. All the presented work has been notified to CISA and the device manufacturer, following a responsible disclosure process. But the manufacturer is still working on mitigation solutions, so we avoid mentioning the manufacturer and device name in this paper. Moreover it is necessary to mention that all the previous processes explained in this article have been created following a black-box approach.

This work also discovered several cybersecurity vulnerabilities. These attacks are only limited due to the communication range allowed by the device since the attacker needs to stay at a distance shorter than 25 meters. Base on our experience the most critical attacks are the ones based on tampering and spoofing of communications. An attacker could generate a fake ECG with a tachycardia or other heart anomaly, like atrial fibrillation, which could make the patient think that he is having a health issue.

Finally, we proposed some possible solutions to these problems. Short-term solutions are based on the location and isolation of the device. Isolation solutions are not a viable long-term solution, as they limit the use of the device to this isolated space. Long-term solutions are usually difficult to apply on IoT devices because they require hardware changes. We suggest implementing properly encrypted data-over-sound communications as a long-term solution.

VIII. Funding & Acknowledgements

This project has received funding from the European Union's Horizon 2020 Research and innovation programme under grant agreement No. 826284.

References

[1] M. Khera, "Think Like a Hacker: Insights on the Latest Attack Vectors (and Security Controls) for Medical Device Applications," *Journal of Diabetes Science and Technology*, vol. 11, no. 2, pp. 207–212, Mar. 2017, publisher: SAGE Publications Inc. [Online]. Available: https://doi.org/10.1177/1932296816677576

[2] J. L. Beavers, M. Faulks, and J. Marchang, "Hacking NHS Pacemakers: A Feasibility Study," in *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, Jan. 2019, pp. 206–212.

[3] E. Marin, D. Singelée, F. D. Garcia, T. Chothia, R. Willems, and B. Preneel, "On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them," in *Proceedings of the 32nd Annual Conference on Computer Security Applications*, ser. ACSAC '16. Association for Computing Machinery, pp. 226–236. [Online]. Available: https://doi.org/10.1145/2991079.2991094

[4] "Medtronic Conexus Radio Frequency Telemetry Protocol (Update C) | CISA." [Online]. Available: https://us-cert.cisa.gov/ics/advisories/ICSMA-19-080-01

[5] "They can hear your heartbeats | Proceedings of the ACM SIGCOMM 2011 conference." [Online]. Available: https://dl.acm.org/doi/abs/10.1145/2018436.2018438

[6] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *2011 Proceedings IEEE INFOCOM*, Apr. 2011, pp. 1862–1870, iSSN: 0743-166X.

[7] M. Rostami, W. Burleson, F. Koushanfar, and A. Juels, "Balancing security and utility in medical devices?" in *Proceedings of the 50th Annual Design Automation Conference*, ser. DAC '13. New York, NY, USA: Association for Computing Machinery, May 2013, pp. 1–6. [Online]. Available: https://doi.org/10.1145/2463209.2488750

[8] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun, "On Limitations of Friendly Jamming for Confidentiality," in *2013 IEEE Symposium on Security and Privacy*, May 2013, pp. 160–173, iSSN: 1081-6011.

[9] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in *Proceedings of the 16th ACM conference on Computer and communications security*, ser. CCS '09. New York, NY, USA: Association for Computing Machinery, Nov. 2009, pp. 410–419. [Online]. Available: https://doi.org/10.1145/1653662.1653712

[10] A. Strielkina, O. Illiashenko, M. Zhydenko, and D. Uzun, "Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment," in *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, May 2018, pp. 67–73.

[11] H. Zhang, G. Wang, M. Lu, D. Wang, and P. Xu, "Emergency Warning and Bidirectional Communication via Digital Audio Broadcast," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 2, pp. 150–159, May 2019, conference Name: IEEE Transactions on Consumer Electronics.

[12] "Sonarax | Contact Tracing & Secure Touch-less Technology." [Online]. Available: https://www.sonarax.com/

[13] R. Rypuła, "robertrypula/AudioNetwork," Apr. 2021, original-date: 2016-04-18T19:42:21Z. [Online]. Available: https://github.com/robertrypula/AudioNetwork

[14] "quiet/quiet," Jun. 2021, original-date: 2016-01-15T00:00:28Z. [Online]. Available: https://github.com/quiet/quiet

[15] kexugit, "Uncover Security Design Flaws Using The STRIDE Approach." [Online]. Available: https://docs.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach

[16] A. Shostack, *Threat Modeling: Designing for Security*, 1st ed. Wiley.

[17] "Audacity." [Online]. Available: https://www.audacityteam.org

[18] "Sonic Visualiser." [Online]. Available: https://www.sonicvisualiser.org/

[19] R. Sharma, K. Kumar, and S. Vig, "DTMF Based Remote Control System," in *2006 IEEE International Conference on Industrial Technology*, Dec. 2006, pp. 2380–2383.

[20] R. Couto, J. Leal, P. M. Costa, and T. Galvão, "Exploring ticketing approaches using mobile technologies: QR codes, NFC and BLE," in *2015 IEEE 18th International Conference on Intelligent Transportation Systems*, pp. 7–12, ISSN: 2153-0017.

[21] P.-Y. Lin, "Distributed secret sharing approach with cheater prevention based on QR code," vol. 12, no. 1, pp. 384–392, conference Name: IEEE Transactions on Industrial Informatics.

[22] G. Starnberger, L. Froihofer, and K. M. Goeschka, "QR-TAN: Secure mobile transaction authentication," in *2009 International Conference on Availability, Reliability and Security*, pp. 578–583.

[23] C.-M. Lee, J.-S. Lin, Y.-P. Hsu, and K.-T. Feng, "Design and Analysis of Optimal Channel-Hopping Sequence for Cognitive Radio Networks," in *2010 IEEE Wireless Communication and Networking Conference*, Apr. 2010, pp. 1–6, iSSN: 1558-2612.

[24] The challenges of developing data over sound technology. [Online]. Available: https://www.sonarax.com/post/why-its-so-challenging-to-develop-data-over-sound-technology-why-the-other-protocols-failed

4.3 Summary of the results of Article 3

This chapter presented the cybersecurity analysis of a specific IoT electrocardiograph, Kardia Mobile [14]. To carefully audit the cybersecurity of the device, first, a thread modelling analysis was performed, using STRIDE methodology [92]. After this preliminary analysis, a process of reversing was applied to understand and detect the technological methods and protocol used by this device. This analysis led to the discovery of a custom protocol base on the use of data-over-sound technologies. Following the characterization of this custom protocol, the IoT device was subject to several cybersecurity tests that led to the successful detection of numerous serious vulnerabilities. Some of these vulnerabilities prove the fact that cybersecurity was omitted in the development and testing process of the device. For example, the device lack any type of encryption in its wireless communications. Allowing the impersonation or information stealing of any measure taken by the device.

All vulnerabilities discovered were subject to a process of responsive disclosure through The Department of Homeland Security's Industrial Control Systems Cyber Emergency Team (ICS-CERT) which transitioned these findings to the Vulnerability Information and Coordination Environment (VINCE) managed by Carnegie Mellon University. Unfortunately, due to the fact, that this is an IoT device most of these vulnerabilities can not be solved without the replacement or change of the product hardware.

Chapter 5

Results and discussion

The previous chapters have shown the research papers that are part of this thesis. In the following sections, the results of each one of them, their relations and answers to the research objectives, previously stated, will be presented.

5.1 Paper 1 - Mobile malware detection using machine learning techniques

The first paper presents the research and creation of a novel method of malware detection focused on detecting mobile PHAs. The proposed detection method made use of supervised machine learning algorithms to identify malicious applications. Unsupervised machine learning algorithms were also tested but showed no relevant results. To distinguish this method from other detection methods previously presented, a scientifically change in the composition of the training dataset was made. Most of the scientific and industry detection algorithms that use machine learning techniques used supervised algorithms, and their training datasets use antivirus engines and other malware detection algorithms as selection criteria [75]. The problem with this methodology is that in end you are replicating the decision model of one or several antivirus engines, rather than creating a new detection method. Moreover, different antivirus engines have shown different criteria and discrepancies when classifying malware or PHAs samples [93][94]. Making the selection of one or several antivirus engines as a selection method a problem.

Unlike these algorithms, the solution presented in the first paper of this thesis used the lifespan of applications as a selection criterion. Using data collected by Tacyt [95], a threat intelligence tool developed by the Telefónica company it is possible to obtain the lifespan of multiple applications published on the Play Store. Querying the Tacyt database it was possible to obtain a dataset of 91,203 mobile applications, that was published on the Google Play Store. Mobile applications removed by Google or its creator in a period of less than a month were considered PHAs. The hypothesis behind this criteria is that legit mobile applications tend to have a longer lifespan than malicious ones. Following this hypothesis, mobile applications with a period life greater than six months were considered benign. To reduce false positives, antivirus engines were involved but only in the process of cleaning possible PHAs. All mobile applications with a period lifespan greater than six months were scanned, and any mobile application detected was removed from the dataset.

Additionally to this process, from each one of the samples collected, a total of 601 features were obtained. All of the features obtained were carefully normalized, and only features that can be present in all possible applications were used. Any, specific features or unique characteristics, such as the usage of IP addresses or specific domains were removed from the dataset. This process, is another differential characteristic of this paper.

Other research papers did not have this normalize process into account and add every possible extracted value as a feature. For example Drebin [75] used 545,000 features versus 601 feature used by this solution.

After the creation of this unique dataset several machine learning algorithms have been tested, to validate the performance of the proposed solution and analyse its results. Among the tested algorithms, Extreme Gradient Boosting presented the best results with an average precision, recall and f1-score of 89%, and Random Forest Classifier with an average precision, recall and f1-score of 90%. These results proved the hypothesis presented by this paper, malicious applications usually have a shorter lifespan in official app markets. And, this training methodology allows the creation of a novel detection method, avoiding the usage of antivirus engines in the creation of PHAs datasets. As a counterpart and limitation, it is necessary to mention that other machine learning models focused on detecting PHAs have obtained a better accuracy, 94% [75] or 95% [31]. Probably an increase in the PHAs used on the dataset will improve its detection rate, and like other machine learning, this model can be continuously retrained. But a 90% accuracy permits the applicability of this detection method.

One way to use this detection method, is to include it as an application control mechanism inside mobile app stores. Whenever a new mobile application is going to be published, it can be scan and stop it publishing if it is categorized as PHA. Furthermore, the improvement of the application control mechanisms applied to app stores will directly benefit all users. Because of these reasons, this research is directly related to the first research goal: The study the usage and development of machine learning techniques to enhance the cybersecurity protection applicable to mobile devices. The development of heterogeneous methods of detection applied to mobile app providers will directly benefit the users of those app markets. That directly affects healthcare centres with BYOD policies, where multiple devices, from vendors and versions, are used. This solution could be generally applied to all android devices that are using the same app store.

Therefore, in relation to the first research goal, The study of the usage and development of machine learning techniques to enhance the cybersecurity protection applicable to mobile devices, the presented results proved the possibility of creating solutions based on machine learning techniques that can be heterogeneously applied. Solutions can be developed, and machine learning can be involved or not, in the creation of Healthcare solutions, but the main requirement is adjusting these solutions to the specific needs of this sector.

5.2 Paper 2 - Analysis of darknets and their connections

The second paper explores, analyze and index data from darknets. This process looked to obtain and detect threats against Healthcare services. Darknets have become an area of illegal activity that can present relevant information to multiple sectors. In this case, the research work was centred on analysing Tor and i2p networks. Tor is the most popular darknet, but darknets such as i2p could also contain relevant information that could help accomplish the second research objective, To analyse the structure of darknets in order to understand criminal activities and threats related to the Healthcare Industry. This research objective also entangles what type of information or how this information is being shared.

First of all, in the process of analyzing darknets, it is necessary to collect information and identify sites relevant that could help answer the second research objective. To perform this activity a darknet crawler capable of collecting and indexing information was developed in the UAH. This crawler obtained a large amount of data that allow the identification of potential threats against Healthcare services. It is necessary to mention, that even though the focus of this research was to study Healthcare data being sold in dark markets, the scientific research successfully led to the discovery of the interconnection between different darknets. Even though it was not the primary focus of this research, this scientific breakthrough was accomplished during this research process.

But during this research process, it was discovered that Tor and i2p networks are interconnected. Multiple references to the Tor network, such as .onion addresses, were found in the i2p network. In order to detail analyze this interconnection graph analysis techniques were used. All the obtained addresses, and darknet services, were used to build a directed graph, removing any surface web links. Using this directed graph network metrics were obtained, proving that the Tor network is more widely used but some sites of these networks are not discovered if i2p is not indexed. Some users only publish certain Tor hidden services addresses in i2p. In summary, some users publish references or information from Tor in i2p and vice-versa. Proving, that anyone looking to obtain or analyze the darknet needs to access and study multiple darknets. Some of the users interested in this anonymity use both, Tor and i2p, of the analyzed networks. This graph analysis also allowed the identification of the most important domains in the network. As mentioned earlier this network is not publicly indexed, and because of that multiple popular sites are indexed sites, webs with a compendium of darknets links. Moreover, due to the fact that such information and links can be useful to other researchers, a free dataset with this information was published. Other researchers or o Law Enforcement Agencies (LEAs) can use this information to perform their own data collection or investigation attempts.

Reaching this point, it is necessary to address some recent events that differentiate the current situation from the previous one. One of the premises of looking into darknets was the premise that cybercriminals were actively using that networks as support to attack target healthcare services. At the moment of writing the paper Interconnection between darknets, beginning in 2020, ransomware was actively used but cybercriminals but had not evolved into a process of double extortion. Following the establishment of Ransomware as a Business (RaaB), [5], since 2021 ransomware has experienced an evolution into a double or triple extortion model. In the origin, cybercriminals encrypted information and then ask for a ransom. Now with a double extortion model cybercriminals stole and encrypt the information. A further step is the triple extortion model, where cybercriminals extort the company affected and its clients. Cybercriminals contact directly with the company clients to ask for a ransom in exchange for not publishing private information, such as healthcare data[96].

In double and triple extortion scenarios if the victims, do not cooperate with the payment the cybercriminals threaten to publish the stolen information on the internet. Is here, where Tor darknet, becomes a key part of this process. Darknets allow anonymously hosts and publish information. Cybercriminal groups associated with ransomware have created their own ”corporate” sites in Tor, where they publish information about their victims and also serve as a communication and negotiation platform with the affected victims. Amongst these victims, several hospitals and healthcare services[88][97] have been affected and their information has been published on Tor. This current situation supports and validates the hypothesis of the use of darknets as a network for publishing and selling stolen healthcare information. Darknets have proved to be a fundamental and necessary part of the RaaB ecosystem.

5.3 Paper 3 - Healthcare devices security

In the third paper, the cybersecurity of medical devices is researched and reviewed, looking to answer the third research objective: The study of the cybersecurity status of modern IoT medical devices. As previously mentioned, in other chapters of this thesis, medical devices involving technology and software have been focused on safety measures. Medical devices centred on diagnosis, treatment and novel IoT devices usually do not comply with any minimal cybersecurity requirements. To prove this statement, the third written paper was focused in perform an independent cybersecurity audit of a medical IoT product used in patient monitoring.

The device chosen to perform this audit was a portable IoT electrocardiograph currently in use by Healthcare centres. No prior knowledge or security concerns were public before performing this analysis. In the context of the ProTego H2020 project[67], where the University of Alcalá took part as a member of the project, several research activities were performed. One of these successful research activities and knowledge transfers was the presentation and explanation of different digital medical devices used by several ProTego member hospitals. Among the presented devices IoT devices were the Kardia mobile electrocardiograph[14]. Being this a small and affordable device it was acquired to be reviewed.

This electrocardiograph is a novel device with unknown technology implementations, and because of that, the research started with a process of reversing engineering and analysis. In this preliminary analysis, it was expected to detect the usage of Bluetooth Low Energy (BLE) or other custom radio frequency protocols but the device performed communications through sound, known as data-over-sound communications. After this analysis, a threat model based on STRIDE framework[92] was built. Following a methodology, such as STRIDE, allow the assessment and test of the most important attacks, covering the attack surface offered by the device.

This process of auditing successfully detected numerous vulnerabilities, that were submitted to a process of responsible disclosure. The vulnerabilities detected allow spoofing, and tampering of any communication with the device, due to the lack of encrypted communications. No mechanism of encryption or integrity was placed in the custom data-over-sound protocol used by the device. This also results in the possibility of performing denial of service attacks. These discoveries support the lack of cybersecurity measures in medical devices. Evidently, the existence of multiple vendors and the enormous ecosystem behind the manufacturing and creation of medical devices, make it impossible to create a general cybersecurity assessment, just taking into account one device. But in the recent times numerous vulnerabilities has been discovered in different medical devices, such as insulin pumps[53][91][98], pacemakers[54][99][100][101] and other devices[55][102][103]. Due to this situation, the European Union has been focusing resources on creating cybersecurity guidelines for medical devices[104], that had led to the creation and appliance of new regulations[105]. Those regulations require the inclusion of cybersecurity requirements in the design and testing of these devices. Unfortunately, even though this regulation will force the inclusion of cybersecurity protections in the manufacturing and design of new devices, does not solve the current lack of security of multiple medical devices currently in use.

It is necessary to clarify, that most of the current technological devices used in diagnosis and treatment use multiple software components. Such as proprietary software, open-source software or an operating system, like any other IoT or technological device. Researching this topic, in 2020 a threat report written by Palo Alto Networks, identified that 83% of medical imaging devices are running on unsupported operating systems[106]. Unfortunately, the operative system layer is usually hidden in those devices and runs as black boxes inside hospitals. IT administrations or other technical personnel usually do not have access to these software components. And even though they have access any update can improve the cybersecurity but compromise the safety of the device, due to software malfunctions.

Force new regulations is a step into add cybersecurity protections to medical devices but does not solve the current situation. It is not possible to replace all current medical devices in use or use only audited devices with proper cybersecurity measures. And even though, theoretically, novel devices will comply with cybersecurity regulations, it will be years before the full replacement of all insecure medical devices. Making it necessary further research on the creation of security solutions that can be applicable to the current medical devices park in use.

Chapter 6

Conclusions and future work

In this thesis, several techniques problems and points of view related to cybersecurity in the Healthcare industry have been presented. The results obtained support and evidence of the cybersecurity needs of this industry, taking into account its unique features and necessities. Because of those results, future research studies can use this thesis as a starting point to understand some of the threats that are currently affecting the Healthcare Industry. Hereafter, the following section presents a summary of the main conclusions obtained during the work of this thesis and possible lines of future work that have been identified.

6.1 Conclusions

The first paper, ”Malware Detection Inside App Stores Based on Lifespan Measurements”, presents research that supports the usage of machine learning detection methods for detecting mobile PHAs that do not involve the usage of antivirus as selection criteria. The usage of lifespan measurements in app stores is only one idea that can be extended or changed in multiple ways. Any detection method that manages to evade the usage of antivirus, and use other malware selection criteria, will create novel detection of methods. On the other hand, one unsolved issue of the solution presented is its applicability to other mobile ecosystems like iOS. Unfortunately, due to the lack of iOS app store data, the solution can not be tested but that does not mean that is not applicable. Following the same idea, used in the creation of the paper dataset, a dataset with iOS App Store information could be created. But only the owner, or someone with access to this data, will be able to develop a solution. Also, it is necessary to take into account that if his experiment is performed will probably generate different results. Due to the fact that the reviewing and publishing policies in the iOS App Store are different than the Android Play Store. But nonetheless, this is a method applicable as a control mechanism in any app store. Methods easily implemented across all healthcare personnel need to be developed, due to the heterogeneous mobile market. One of the principles repeatedly reiterated in this thesis is the development and research of applicable methods. That could make sense in almost any research scenario, but in Healthcare research is indispensable the collaboration and advisory of healthcare institutions. The particularities in its daily operations and management make crucial its advisory in any developed methods.

In the second paper, ”Interconnection between darknets”, a graph analysis of i2p and Tor networks is presented. This analysis is performed using a freely accessible dataset, created in the context of this research, that links Tor hidden services with i2p eepsites. Proving the relation between different darknets and their current use by multiple users. In order to discover more information, it is necessary to access other similar anonymous technologies. I2p and Tor share a user base in common that lead to the exchange of link sites and relevant information. This will probably affect other darknets such as Freenet [107] or ZeroNet [108]. Anyone interested in obtaining as much information as possible from the Tor network should also explore other darknets looking for hidden services references. Furthermore, as mentioned earlier, this discovery was not the main idea of this research and was subsequently discovered during a process of scientific research.

That does not mean this line of research should be discarded. As mentioned before, following the establishment of Ransomware as a Business (RaaB) [5], since 2021 ransomware gangs have increased the usage of the Tor network. Tor network offers a platform to publish stolen information anonymously, for sale or as a method of double extortion. This situation supports the necessity of research and monitoring of darknets, to discover and detect threats. And this is directly related to healthcare data and services,[88][97]. Furthermore, several of the victims publicised by these groups have turned out to be health services [16][17], proving the need and interest in the study and monitoring of such networks.

In the third paper, "Security and privacy issues of data-over-sound technologies used in IoT healthcare devices", a security analysis of a medical IoT device is performed and presented. Applying STRIDE threat analysis methodology multiple attacks were assessed, leading to the discovery of multiple critical vulnerabilities. These discoveries, even though only one device was analyzed, tend to support the hypothesis of the lack of cybersecurity measures in multiple medical devices. The analyzed device was not submitted to any previous cybersecurity reviews, multiple vulnerabilities were easily identifiable. Furthermore, this also demonstrates the lack of cybersecurity involvement in all the development phases of the products. Terms such as security by design were totally oblivious to the development and design of the product. All this further demonstrates the lack of cybersecurity regulations and controls over medical products. The European Union has tried to legislate in this aspect[105]. But unfortunately, the majority of the current devices currently in use have not been subjected to this legislation. Due to this situation, multiple medical devices probably present minimal or no cybersecurity features. The usage of medical devices and their lack of cybersecurity features is one of the biggest threats and problems to the healthcare industry, hindering any process of modernisation and the cybersecurity needs of medical facilities. Moreover, there is not a currently easily applicable solution to this aspect. A software solution is difficult or impossible to design because some cybersecurity failures are hardware related. And in top of that it is not easy to replace, and in most cases is not possible, a medical product with another security design. The usage of medical devices with cybersecurity features by healthcare services will probably be a process that will not be achieved in years but decades. Probably, only demanding a strong legislation in cybersecurity aspects will force manufacturers to include cybersecurity as a need in their design and development process. Medical devices should be submitted to product certification and evaluation process (e.g., LINCE [109], BSPA [110], CSPN [111]), or a specific certification specially design for medical devices.

6.2 Future work

Following the discussion of the results and conclusions previously exposed, several lines of future work can be explored. Cybersecurity applicable to the Healthcare Industry is a huge field of research, but taking into account the obtained knowledge from this thesis, several future research lines could be:

- In relation to the design of novel methods of malware detection, one line of work easily extended is the development of detection methods that avoid the usage of antivirus as selection criteria. The development of novel criteria as selection methods of PHAs or malware is a line of research that could lead to promising research differential and complementary detection methods.
- In relation to the development of multi-platform cybersecurity solutions for the mobile ecosystem. At the moment of writing this thesis, a unification of the mobile ecosystem seems distant or highly improbable. Any advance in developing heterogeneous solutions can be considered a research breakthrough. Furthermore, the mobile ecosystem is far from disappearing and now it is being extended and increased by the usage of IoT devices.

- In relation to possible transition contingency measures. As mentioned earlier the usage of medical devices with cybersecurity features by healthcare services will probably be a process that will not be achieved in years but decades. Multi-platform solutions can contribute as a contingency measure, but it is necessary to develop further tools and techniques in this area. Transition solutions capable of offering cybersecurity services need to be developed and applied in the current industry.
- In relation to darknets analysis, it is necessary to study and monitor ransomware leak sites accessible through Tor. RaaB operators are using darknets as a method of maintaining anonymity. But multiple research works can be developed using the published information on those sites (e.g., monitor publication dates, analyse and classified published victims and analyse leaked data).
- Further cybersecurity analysis of other medical devices. Only one medical device was analysed in the context of this thesis. The cybersecurity review of other medical devices will probably lead to the discovery of multiple security vulnerabilities. These discoveries could also lead to the creation of possible solutions and protection methods. The European Commission is supporting this idea and is currently looking to fund projects that analyse and improve the security of medical devices under the Horizon Europe research framework program [66].
- Following the cybersecurity needs of the Healthcare Industry, it is required to develop the necessary legal frameworks and Information Security Management Systems. This development of legislation, frameworks and methodologies is a combined effort between technological and legal people, that needs to be further developed. For example, a specific cybersecurity certification for medical devices can be designed, or existing ones can be adapted.

Bibliography

[1] W. H. Ware, "Security and privacy in computer systems," in *Proceedings of the April 18-20, 1967, spring joint computer conference*, ser. AFIPS '67 (Spring). New York, NY, USA: Association for Computing Machinery, Apr. 1967, pp. 279–282. [Online]. Available: https://doi.org/10.1145/1465482.1465523

[2] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, "Cutting the gordian knot: A look under the hood of ransomware attacks," in *International conference on detection of intrusions and malware, and vulnerability assessment.* Springer, 2015, pp. 3–24.

[3] S. Mansfield-Devine, "Ransomware: the most popular form of attack," *Computer Fraud & Security*, vol. 2017, no. 10, pp. 15–20, 2017.

[4] "Financial Trend Analysis," p. 17. [Online]. Available: https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf

[5] N. Kshetri and J. Voas, "Ransomware as a business (raab)," *IT Professional*, vol. 24, no. 02, pp. 83–87, mar 2022.

[6] "Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas." p. 11. [Online]. Available: https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf

[7] S. Ghafur, E. Grass, N. R. Jennings, and A. Darzi, "The challenges of cybersecurity in health care: the uk national health service as a case study," *The Lancet Digital Health*, vol. 1, no. 1, pp. e10–e12, 2019.

[8] M. Moran Stritch, M. Winterburn, and F. Houghton, "The conti ransomware attack on healthcare in ireland: Exploring the impacts of a cybersecurity breach from a nursing perspective," *Canadian Journal of Nursing Informatics*, vol. 16, no. 3-4, 2021.

[9] T. Anderson and W. Torreggiani, "The impact of the cyberattack on radiology systems in ireland," *Irish Medical Journal*, vol. 114, no. 5, p. 137, 2021.

[10] P. Muncaster, "Infant Fatality Could Be First Recorded Ransomware Death," Oct. 2021. [Online]. Available: https://www.infosecurity-magazine.com/news/infant-first-ransomware-death/

[11] S. Jayakumar, "Singhealth cyber attack: Learning from coi findings," 2019.

[12] B. Meskó, Z. Drobni, É. Bényei, B. Gergely, and Z. Győrffy, "Digital health is a cultural transformation of traditional healthcare," *Mhealth*, vol. 3, 2017.

[13] "Darknet: Geopolitics and Uses | Wiley." [Online]. Available: https://www.wiley.com/en-us/Darknet%3A+Geopolitics+and+Uses-p-9781119522492

[14] "Kardia Mobile ECG - Alivecor - electrocardiograma para IOS y Android." [Online]. Available: https://tienda.alivehs.com/es/inicio/8-kardia-mobile.html

[15] "The Tor Project | Privacy & Freedom Online." [Online]. Available: https://torproject.org

[16] "FBI releases alert about Hive ransomware after attack on hospital system in Ohio and West Virginia." [Online]. Available: https://www.zdnet.com/article/fbi-releases-alert-about-hive-ransomware-after-attack-on-hospital-system/

[17] "karakurt-threat-profile-analyst-note.pdf." [Online]. Available: https://www.hhs.gov/sites/default/files/karakurt-threat-profile-analyst-note.pdf

[18] . M. S. S. Monica and C. 90401-3208, "Willis H. Ware - Publications," Tech. Rep. [Online]. Available: https://www.rand.org/pubs/authors/w/ware_willis_h.html

[19] B. Peters, "Security considerations in a multi-programmed computer system," in *Proceedings of the April 18-20, 1967, spring joint computer conference*, ser. AFIPS '67 (Spring). New York, NY, USA: Association for Computing Machinery, Apr. 1967, pp. 283–286. [Online]. Available: https://doi.org/10.1145/1465482.1465524

[20] S. P. Marsh, "Formalising Trust as a Computational Concept," p. 184.

[21] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," National Institute of Standards and Technology, Tech. Rep., Aug. 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[22] F. M. Avolio, M. J. Ranum, and M. Glenwood, "A network perimeter with secure external access," in *Proceedings of the Internet Society Symposium on Network and Distributed System Security*, 1994, pp. 109–119.

[23] K. Dadheech, A. Choudhary, and G. Bhatia, "De-militarized zone: a next level to network security," in *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*. IEEE, 2018, pp. 595–600.

[24] N. Wagner, C. Ş. Şahin, M. Winterrose, J. Riordan, J. Pena, D. Hanson, and W. W. Streilein, "Towards automated cyber decision support: A case study on network segmentation for security," in *2016 IEEE Symposium Series on Computational Intelligence (SSCI)*. IEEE, 2016, pp. 1–10.

[25] T. Verwoerd and R. Hunt, "Intrusion detection techniques and approaches," *Computer communications*, vol. 25, no. 15, pp. 1356–1365, 2002.

[26] F. Sabahi and A. Movaghar, "Intrusion detection: A survey," in *2008 Third International Conference on Systems and Networks Communications*. IEEE, 2008, pp. 23–26.

[27] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[28] J.-h. Li, "Cyber security meets artificial intelligence: a survey," *Frontiers of Information Technology & Electronic Engineering*, vol. 19, no. 12, pp. 1462–1474, 2018.

[29] N. N. A. Sjarif, S. Chuprat, M. N. Mahrin, N. A. Ahmad, A. Ariffin, F. M. Senan, N. A. Zamani, and A. Saupi, "Endpoint detection and response: Why use machine learning?" in *2019 International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 2019, pp. 283–288.

[30] S. Omar, A. Ngadi, and H. H. Jebur, “Machine learning techniques for anomaly detection: an overview,” *International Journal of Computer Applications*, vol. 79, no. 2, 2013.

[31] J. Sahs and L. Khan, “A machine learning approach to android malware detection,” in *2012 European Intelligence and Security Informatics Conference.* IEEE, 2012, pp. 141–147.

[32] D. Gavriluţ, M. Cimpoeşu, D. Anton, and L. Ciortuz, “Malware detection using machine learning,” in *2009 International Multiconference on Computer Science and Information Technology.* IEEE, 2009, pp. 735–741.

[33] M. Crawford, T. M. Khoshgoftaar, J. D. Prusa, A. N. Richter, and H. Al Najada, “Survey of review spam detection using machine learning techniques,” *Journal of Big Data*, vol. 2, no. 1, pp. 1–24, 2015.

[34] P. Bhatt and P. H. Rughani, “Machine learning forensics: A new branch of digital forensics.” *International Journal of Advanced Research in Computer Science*, vol. 8, no. 8, 2017.

[35] A. Hobbs, *The colonial pipeline hack: Exposing vulnerabilities in us cybersecurity.* SAGE Publications: SAGE Business Cases Originals, 2021.

[36] M. Conti, A. Gangwal, and S. Ruj, “On the economic significance of ransomware campaigns: A bitcoin transactions perspective,” *Computers & Security*, vol. 79, pp. 162–189, 2018.

[37] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, “Cybersecurity for industrial control systems: A survey,” *computers & security*, vol. 89, p. 101677, 2020.

[38] W. Yue, Z. Wang, H. Chen, A. Payne, and X. Liu, “Machine learning with applications in breast cancer diagnosis and prognosis,” *Designs*, vol. 2, no. 2, p. 13, 2018.

[39] A. L. Beam and I. S. Kohane, “Big data and machine learning in health care,” *Jama*, vol. 319, no. 13, pp. 1317–1318, 2018.

[40] M. M. Archibald and A. Barnard, “Futurism in nursing: Technology, robotics and the fundamentals of care,” *Journal of Clinical Nursing*, vol. 27, no. 11-12, pp. 2473–2480, 2018.

[41] E. R. Dorsey and E. J. Topol, “State of telehealth,” *New England journal of medicine*, vol. 375, no. 2, pp. 154–161, 2016.

[42] “Health Care & Social Assistance in the U.S. 2021.” [Online]. Available: https://www.statista.com/study/15826/health-care-and-social-assistance-in-the-us/

[43] “U.S. Digital Health Market Size Report, 2022-2030.” [Online]. Available: https://www.grandviewresearch.com/industry-analysis/us-digital-health-market-report

[44] I. C. I. CYBERSECURITY, “Executive order–improving critical infrastructure cybersecurity,” 2013.

[45] C. I. Cybersecurity, “Framework for improving critical infrastructure cybersecurity,” *Framework*, vol. 1, no. 11, 2014.

[46] M. P. Barrett *et al.*, “Framework for improving critical infrastructure cybersecurity,” *National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep*, 2018.

[47] N. Abouzakhar, “Critical infrastructure cybersecurity: A review of recent threats and violations,” 2013.

[48] J. J. Chung, “Critical infrastructure, cybersecurity, and market failure,” *Or. L. Rev.*, vol. 96, p. 441, 2017.

[49] C. S. Kruse, B. Frederick, T. Jacobson, and D. K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends," *Technology and Health Care*, vol. 25, no. 1, pp. 1–10, 2017.

[50] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, 2018.

[51] A. J. Coronado and T. L. Wong, "Healthcare cybersecurity risk management: Keys to an effective plan," *Biomedical instrumentation & technology*, vol. 48, no. s1, pp. 26–30, 2014.

[52] E. Marin, D. Singelée, F. D. Garcia, T. Chothia, R. Willems, and B. Preneel, "On the (in) security of the latest generation implantable cardiac defibrillators and how to secure them," in *Proceedings of the 32nd annual conference on computer security applications*, 2016, pp. 226–236.

[53] W. Alexander, "Barnaby Jack Could Hack Your Pacemaker and Make Your Heart Explode," Jun. 2013. [Online]. Available: https://www.vice.com/en/article/avnx5j/i-worked-out-how-to-remotely-weaponise-a-pacemaker

[54] "Medtronic Conexus Radio Frequency Telemetry Protocol (Update C) | CISA." [Online]. Available: https://www.cisa.gov/uscert/ics/advisories/ICSMA-19-080-01

[55] "NVD - CVE-2020-15485." [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2020-15485

[56] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "Imdguard: Securing implantable medical devices with the external wearable guardian," in *2011 Proceedings IEEE INFOCOM*. IEEE, 2011, pp. 1862–1870.

[57] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," in *Proceedings of the ACM SIGCOMM 2011 conference*, 2011, pp. 2–13.

[58] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for scada systems," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1836–1846, 2008.

[59] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for scada systems," *Computers & security*, vol. 56, pp. 1–27, 2016.

[60] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Power system reliability evaluation with scada cybersecurity considerations," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1707–1721, 2015.

[61] Z. Zhang, "Cybersecurity policy for the electricity sector: the first step to protecting our critical infrastructure from cyber threats," *BUJ Sci. & Tech. L.*, vol. 19, p. 319, 2013.

[62] C. Laughlin, "Cybersecurity in critical infrastructure sectors: A proactive approach to ensure inevitable laws and regulations are effective," *Colo. Tech. LJ*, vol. 14, p. 345, 2015.

[63] A. Strielkina, O. Illiashenko, M. Zhydenko, and D. Uzun, "Cybersecurity of healthcare iot-based systems: Regulation and case-oriented assessment," in *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*. IEEE, 2018, pp. 67–73.

[64] "Funding & tenders. toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures." [Online]. Available: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/su-tds-02-2018

[65] “Funding & tenders. raising awareness and developing training schemes on cybersecurity in hospitals.” [Online]. Available: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/su-tds-03-2018

[66] “Funding & tenders. enhancing cybersecurity of connected medical devices.” [Online]. Available: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-hlth-2022-ind-13-01

[67] “Data-protection toolkit reducing risks in hospitals and care centers | ProTego Project | Fact Sheet | H2020 | CORDIS | European Commission.” [Online]. Available: https://cordis.europa.eu/project/id/826284

[68] G. Martin, P. Martin, C. Hankin, A. Darzi, and J. Kinross, “Cybersecurity and healthcare: how safe are we?” *BMJ*, vol. 358, p. j3179, Jul. 2017, publisher: British Medical Journal Publishing Group Section: Analysis. [Online]. Available: https://www.bmj.com/content/358/bmj.j3179

[69] L. Coventry and D. Branley, “Cybersecurity in healthcare: A narrative review of trends, threats and ways forward,” *Maturitas*, vol. 113, pp. 48–52, Jul. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378512218301658

[70] C. S. Kruse, B. Frederick, T. Jacobson, and D. K. Monticone, “Cybersecurity in healthcare: A systematic review of modern threats and trends,” *Technology and Health Care*, vol. 25, no. 1, pp. 1–10, Jan. 2017, publisher: IOS Press. [Online]. Available: https://content.iospress.com/articles/technology-and-health-care/thc1263

[71] “Office for the Advancement of Telehealth,” Apr. 2017, last Modified: 2021-12-23T10:47-05:00. [Online]. Available: https://www.hrsa.gov/rural-health/telehealth

[72] “Coronavirus.” [Online]. Available: https://www.who.int/health-topics/coronavirus

[73] “Annual mobile app downloads worldwide by store 2025.” [Online]. Available: https://www.statista.com/statistics/1010716/apple-app-store-google-play-app-downloads-forecast/

[74] D. Maier, T. Müller, and M. Protsenko, “Divide-and-conquer: Why android malware cannot be stopped,” in *2014 Ninth International Conference on Availability, Reliability and Security*. IEEE, 2014, pp. 30–39.

[75] D. Arp, M. Spreitzenbarth, M. Hubner, H. Gascon, K. Rieck, and C. Siemens, “Drebin: Effective and explainable detection of android malware in your pocket.” in *Ndss*, vol. 14, 2014, pp. 23–26.

[76] “NCSC: National Cyber Security Centre - ransomware attack on health sector.” [Online]. Available: https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf

[77] “Cyberattack hits major hospital system, possibly one of the largest in U.S. history.” [Online]. Available: https://www.nbcnews.com/tech/security/cyberattack-hits-major-u-s-hospital-system-n1241254

[78] “Public Report of the Committee of Inquiry (COI) into the cyber attack on Singapore Health Services Private Limited Patient Database.” [Online]. Available: https://www.mci.gov.sg/-/media/mcicorp/doc/report-of-the-coi-into-the-cyber-attack-on-singhealth-10-jan-2019.ashx

[79] L. Ablon, M. C. Libicki, and A. A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers’ Bazaar*. Rand Corporation, Mar. 2014, google-Books-ID: LgBOAwAAQBAJ.

[80] "Understanding Password Choices: How Frequently Entered Passwords Are Re-used across Websites | USENIX." [Online]. Available: https://www.usenix.org/conference/soups2016/technical-sessions/presentation/wash

[81] H. Berghel, "Identity theft, social security numbers, and the Web," *Communications of the ACM*, vol. 43, no. 2, pp. 17–21, Feb. 2000. [Online]. Available: https://doi.org/10.1145/328236.328114

[82] T. J. Holt, O. Smirnova, and Y. T. Chua, "Exploring and Estimating the Revenues and Profits of Participants in Stolen Data Markets," *Deviant Behavior*, vol. 37, no. 4, pp. 353–367, Apr. 2016, publisher: Routledge _eprint: https://doi.org/10.1080/01639625.2015.1026766. [Online]. Available: https://doi.org/10.1080/01639625.2015.1026766

[83] T. J. Holt, "Exploring the social organisation and structure of stolen data markets," *Global Crime*, vol. 14, no. 2-3, pp. 155–174, May 2013, publisher: Routledge _eprint: https://doi.org/10.1080/17440572.2013.787925. [Online]. Available: https://doi.org/10.1080/17440572.2013.787925

[84] D. McCoy, K. Bauer, D. Grunwald, T. Kohno, and D. Sicker, "Shining Light in Dark Places: Understanding the Tor Network," in *Privacy Enhancing Technologies*, ser. Lecture Notes in Computer Science, N. Borisov and I. Goldberg, Eds. Berlin, Heidelberg: Springer, 2008, pp. 63–76.

[85] "I2P Anonymous Network." [Online]. Available: https://geti2p.net/en/

[86] "Ahmia — Search Tor Hidden Services." [Online]. Available: https://ahmia.fi/

[87] "Onion Search Engine." [Online]. Available: https://www.onionsearchengine.com/

[88] U. D. of Health and H. S. O. of Information Security, "Lockbit ransomware," https://www.hhs.gov/sites/default/files/lockbit-ransomware.pdf.

[89] N. Leveson and C. Turner, "An investigation of the Therac-25 accidents," *Computer*, vol. 26, no. 7, pp. 18–41, Jul. 1993, conference Name: Computer.

[90] L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville, L. M. R. Arbiza, F. Carbone, M. Marotta, and J. J. C. de Santanna, "Internet of Things in healthcare: Interoperatibility and security issues," in *2012 IEEE International Conference on Communications (ICC)*, Jun. 2012, pp. 6121–6125, iSSN: 1938-1883.

[91] "NVD - CVE-2020-10627." [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2020-10627

[92] ""The Threats to Our Products"," Aug. 2009. [Online]. Available: https://www.microsoft.com/security/blog/2009/08/27/the-threats-to-our-products/

[93] I. Gashi, V. Stankovic, C. Leita, and O. Thonnard, "An experimental study of diversity with off-the-shelf antivirus engines," in *2009 Eighth IEEE International Symposium on Network Computing and Applications*. IEEE, 2009, pp. 4–11.

[94] M. Hurier, K. Allix, T. F. Bissyandé, J. Klein, and Y. Le Traon, "On the lack of consensus in anti-virus decisions: Metrics and insights on building ground truths of android malware," in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 2016, pp. 142–162.

[95] "Tacyt | Telefonica." [Online]. Available: https://www.movistar.cl/web/corporaciones/seguridad/seguridad-de-la-informacion/tacyt

[96] “Finland therapy patients blackmailed after data breach - CNN.” [Online]. Available: https://edition.cnn.com/2020/10/27/tech/finland-therapy-patients-blackmailed-data-breach-intl/index.html

[97] “Conti Ransomware Attacks Impact Healthcare and First Responder Networks,” p. 4.

[98] “NVD - CVE-2019-10964.” [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-10964

[99] “NVD - CVE-2017-12716.” [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-12716

[100] “NVD - CVE-2017-12714.” [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-12714

[101] “NVD - CVE-2017-12712.” [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-12712

[102] “NVD - CVE-2021-27410.” [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2021-27410

[103] “NVD - CVE-2020-27282.” [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2020-27282

[104] “DocsRoom - European Commission.” [Online]. Available: https://ec.europa.eu/docsroom/documents/41863

[105] “Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.),” Apr. 2017, legislative Body: CONSIL, EP. [Online]. Available: http://data.europa.eu/eli/reg/2017/745/oj/eng

[106] “2020 Unit 42 IoT Threat Report 2020 Unit 42 IoT Threat Report,” Mar. 2020. [Online]. Available: https://unit42.paloaltonetworks.com/iot-threat-report-2020/

[107] “Freenet.” [Online]. Available: https://freenetproject.org/index.html

[108] “ZeroNet: Decentralized websites using Bitcoin cryptography and the BitTorrent network.” [Online]. Available: https://zeronet.io/

[109] C. C. Nacional, “Metodología de evaluación para la certificación nacional esencial de seguridad (lince).” [Online]. Available: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/2000-organismo-de-certificacion/4557-ccn-stic-2002-metodologia-de-evaluacion-para-la-certificacion-nacional-esencial-de-seguridad-lince/file.html

[110] M. van Binnenlandse Zaken en Koninkrijksrelaties, “Baseline security product assessment (bspa).” [Online]. Available: https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2020/07/15/nbv-brochure-bspa/Baseline+Security+Product+Assessment+-+BSPA+van+het+NBV.pdf

[111] “Certification CSPN.” [Online]. Available: https://www.ssi.gouv.fr/administration/produits-certifies/cspn/