Revista Facultad de Ingeniería

Journal Homepage: https://revistas.uptc.edu.co/index.php/ingenieria

Information Management Security Vulnerabilities in Smartphones Used by University Students: A Case Study in the Southwest of Colombia

Cristian-Camilo Ordoñez-Quintero[1]

Hugo-Armando Ordoñez-Eraso[2]

Jose-Armando Ordoñez-Córdoba[3]

Received: November 02, 2021 **Accepted:** February 28, 2022 **Published:** March 14, 2022

Citation:

C.-C. Ordoñez-Quintero, H.-A. Ordoñez-Eraso, J.-A. Ordoñez-Córdoba, "Information Management Security Vulnerabilities in Smartphones Used by University Students: A Case Study in the Southwest of Colombia," *Revista Facultad de Ingeniería*, vol. 31 (59), e13957, 2022. https://doi.org/10.19053/01211129.v31.n59.2022.13957

[1] M. Sc. Fundación Universitaria de Popayán (Popayán-Cauca, Colombia). camilo.ordonez@docente.fup.edu.co. ORCID: 0000-0003-4157-1611

[2] Ph. D. Universidad del Cauca (Popayán-Cauca, Colombia). hugoordonez@unicauca.edu.co ORCID: 0000-0002-3465-5617

[3] Ph. D. Universidad del Cauca (Popayán-Cauca, Colombia). jordonez@unicauca.edu.co. ORCID: 0000-0001-6544-0283

Abstract

Currently, students who use smartphones are affected by theft and information leakage, to address this problem, this research aims to identify security vulnerabilities in these devices. In addition, an application to prevent phishing and information leakage was implemented. Effectiveness and performance tests were carried out to identify vulnerabilities and to alert users about them. The threats identified in Android smartphones used by university students in the southwest of Colombia were based on various techniques (phishing, DNS poisoning, identity theft, Man in the middle, foot-printing, spyware). To reach this result, we defined the problem, then we made a literature review, after that we defined the study population, methods, and instruments; finally, we collected the information and analyzed the results. An application was launched to show the security vulnerabilities of malicious software installation, which extracts information from student's devices and makes the security of our mobile phones a priority nowadays; and to achieve greater security on Android smartphones. However, it is essential to be aware of the importance of self-care.

Keywords: android; information leak; mobile devices; phishing; vulnerabilities.

Vulnerabilidades de seguridad en la gestión de la información en teléfonos inteligentes utilizados por estudiantes universitarios: Un estudio de caso en el suroeste de Colombia

Resumen

Actualmente, los estudiantes que utilizan teléfonos inteligentes se ven afectados por el robo y la fuga de información, para abordar este problema, esta investigación tiene como objetivo identificar las vulnerabilidades de seguridad en estos dispositivos. Además, se implementó una aplicación para prevenir el phishing y la fuga de información. Se realizaron pruebas de efectividad y rendimiento para identificar vulnerabilidades y alertar a los usuarios sobre las mismas. Las amenazas identificadas en los teléfonos inteligentes Android utilizados por estudiantes universitarios del suroeste de Colombia se basaron en diversas técnicas (phishing, envenenamiento de DNS, robo de identidad, Man in the middle, foot-printing,

spyware). Para llegar a este resultado, definimos el problema, luego hicimos una revisión de la literatura, luego definimos la población de estudio, métodos e instrumentos; finalmente, recolectamos la información y analizamos los resultados. Se lanzó una aplicación para mostrar las vulnerabilidades de seguridad de la instalación de software malicioso, que extrae información de los dispositivos de los estudiantes y hace que la seguridad de nuestros teléfonos móviles sea una prioridad en la actualidad; y para conseguir una mayor seguridad en los smartphones Android. Sin embargo, es fundamental ser conscientes de la importancia del autocuidado.

Palabras clave: androide; dispositivos móviles; fuga de información; suplantación de identidad; vulnerabilidades.

Vulnerabilidades de segurança na gestão da informação em smartphones usados por estudantes universitários: Um estudo de caso no sudoeste da Colômbia

Resumo

Atualmente, os alunos que utilizam smartphones são acometidos por furtos e vazamento de informações, para solucionar esse problema, esta pesquisa tem como objetivo identificar vulnerabilidades de segurança nesses dispositivos. Além disso, foi implementado um aplicativo para evitar phishing e vazamento de informações. Foram realizados testes de eficácia e desempenho para identificar vulnerabilidades e alertar os usuários sobre elas. As ameaças identificadas em smartphones Android usados por estudantes universitários no sudoeste da Colômbia foram baseadas em várias técnicas (phishing, envenenamento de DNS, roubo de identidade, Man in the middle, foot-printing, spyware). Para chegar a esse resultado, definimos o problema, em seguida fizemos uma revisão de literatura, em seguida definimos a população do estudo, métodos e instrumentos; finalmente, coletamos as informações e analisamos os resultados. Foi lançado um aplicativo para mostrar as vulnerabilidades de segurança da instalação de software malicioso, que extrai informações dos dispositivos dos alunos e torna a segurança de nossos celulares uma prioridade nos dias de hoje; e para obter maior segurança em

smartphones Android. No entanto, é fundamental ter consciência da importância do autocuidado.

Palavras-chave: andróide; dispositivos móveis; phishing; vazamento de informações; vulnerabilidades.

I. INTRODUCTION

Recent studies show that the use of smartphones in Colombia continues to rise. Currently, 96% Colombians use a mobile phone in their daily life [1], most of them are used to store personal information such as photos, videos, bank accounts, and confidential documents of their companies [2]. Incidents related to information theft from mobile devices affecting ordinary citizens decreased by 35% between 2014 and 2016, while attacks to businesses had an increase of more than 20% [3]. This affects many people and has consequences on a psychological, physical, and financial level. One of the most vulnerable groups are university students, who store personal information and conduct transactions in their mobile devices using free and insecure public networks [4]. This article presents an investigation with students from various universities in the southwest of Colombia to identify the risk their mobile devices are exposed to.

GDroid [6] is a tool to detect malware or vulnerabilities in Android, to do so, it uses convolutional neural networks (CNN) to map Android APIs and applications into a heterogeneous graph, then a node classification task is carried out based on the invocations to the Android API and the Usage Patterns. TC-Droid [7] presents a framework that feeds on the text sequence of the application reports generated by AndroPyTool and applies CNN to explore them. In [8], a CCN-based malware detection model that uses an Android application's operation code sequence is presented, to do so, Dreblin´s dataset is used [9].

DCDroid [10] offers a tool to detect vulnerabilities by combining static and dynamic analysis. In the static analysis, it focuses on identifying several types of vulnerabilities in application code snippets. In the dynamic analysis, it prioritizes activation of user interface (UI) components based on static analysis results to confirm SSL / TLS misuse.

As can be seen in the related works, existing approaches are based on neural network models with very good results in the classification of malware; however, none of them study the behavior of real users directly to identify the most frequent vulnerabilities.

The remainder of this article is organized as follows: Section II presents the case study and the mobile application developed; Section III exposes the results; and Section IV presents the conclusions and future work.

II. Case Study

The case study is descriptive/holistic, and it is based on Runeson's methodology (Figure 1) [11]. The main objective is to identify the vulnerability of mobile devices with the Android operating system used by university students from the southwest of Colombia.

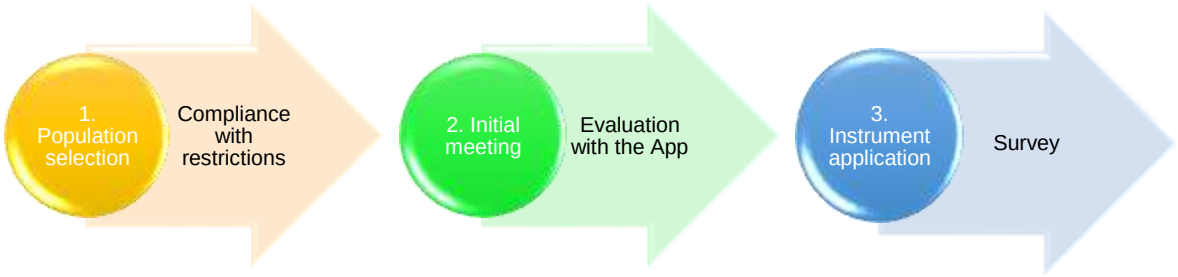

Fig. 1. Case study phases

A. Selection of the Study Population

The population is made up of university students between 16 - 25 years old because of their vulnerability; many times, they do not have precaution when connecting to free Wi-Fi networks or providing information, thus leading to information or credentials theft. The students use a smartphone with Android operating system. The population consists of 129 participants and is described in Figure 2.

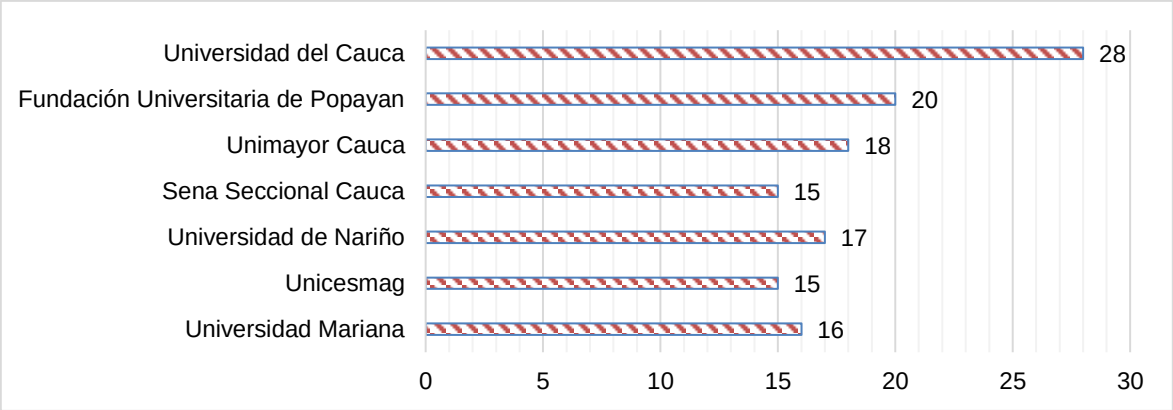

Fig. 2. University Students from the southwest of Colombia.

B. Compliance with Restrictions

Information about Android vulnerabilities from version 5.0 to 10.0 is collected from the National Vulnerability Database (NVD) provided by the National Institute of Standards and Technology [12].

C. Initial Meeting

Vulnerabilities, severity, and details are classified using the analyzed data. On August 28 and 29, 2020, two meetings were held via Zoom: one meeting with 70 people and another with 59 for a total of 129 students from different universities.

D. Evaluation with the App

The analysis unit corresponds to the execution of the process, that is, the installation of the application on the devices by a cybersecurity expert, thus measuring qualitative and quantitative aspects. At a quantitative level, the vulnerability identification time was considered, and for the qualitative aspect, through the evaluation of the expert, it was determined to what degree the devices are vulnerable. Table 1 shows the results of the versions found and the app installation messages.

Table 1. Android Versions.

Version	Number of devices	Message during installing
ANDROID 5	10	Message configuration during installation

Version	Number of devices	Message during installing
ANDROID 7	15	Automatically installed
ANDROID 8	40	Confirmation Message during installation
ANDROID 9	30	Message configuration during installation
ANDROID 10	34	Message configuration during installation
TOTAL	129	

E. Application of Validation Instruments

Surveys were used as information collection methods. Two vulnerability identification cycles were defined to establish how the repetition of the execution process affects the results obtained. At the end of the two cycles, it was decided to conduct a survey to each participating student about the process and implementation of the application.

F. Mobile Application

To conduct the case study, it was necessary to develop an application named Android Protect. It has the functionality of identifying whether there are vulnerabilities in the mobile device it was installed to, then each of its components is shown.

Fig. 3. Application icon.

Figure 4 shows the application toolbar which illustrates the icons of each module. The first icon from left to right is a key, which represents the configuration module; the second is a circle and it is one of the most important because it scans the vulnerabilities according to the version used in the mobile device; the third icon shows sheets and graphs, it is the results module that shows the terms related to the configurations and scans of the vulnerabilities in a clear way and with a brief description, in addition to the most common attack; finally, the fourth icon is a light bulb, which provides some alternatives as a solution to counteract data leaks. In

addition, the sources from which the registered vulnerabilities are extracted in real time according to the version of each device are detailed with a brief description of each menu. In module 1, when entering the application, it asks the user for permissions, which are shown below.

The first module of the application verifies if the mobile device is with Root access, that is, released with all the permissions to use the device. Module 2 is the most important as it generates the device's scanner, it has a table of 3 items which categorizes the scanned information for a better understanding, this is done in technical terms which help to know the severity, the description of the vulnerability, and the code of the vulnerability. The scanning process is done using the Web Scraping technique, which consists of capturing the vulnerabilities registered by the manufacturers in a table according to the Android version of the device, then the application shows the results of the scan. Module 3 displays the vulnerabilities.

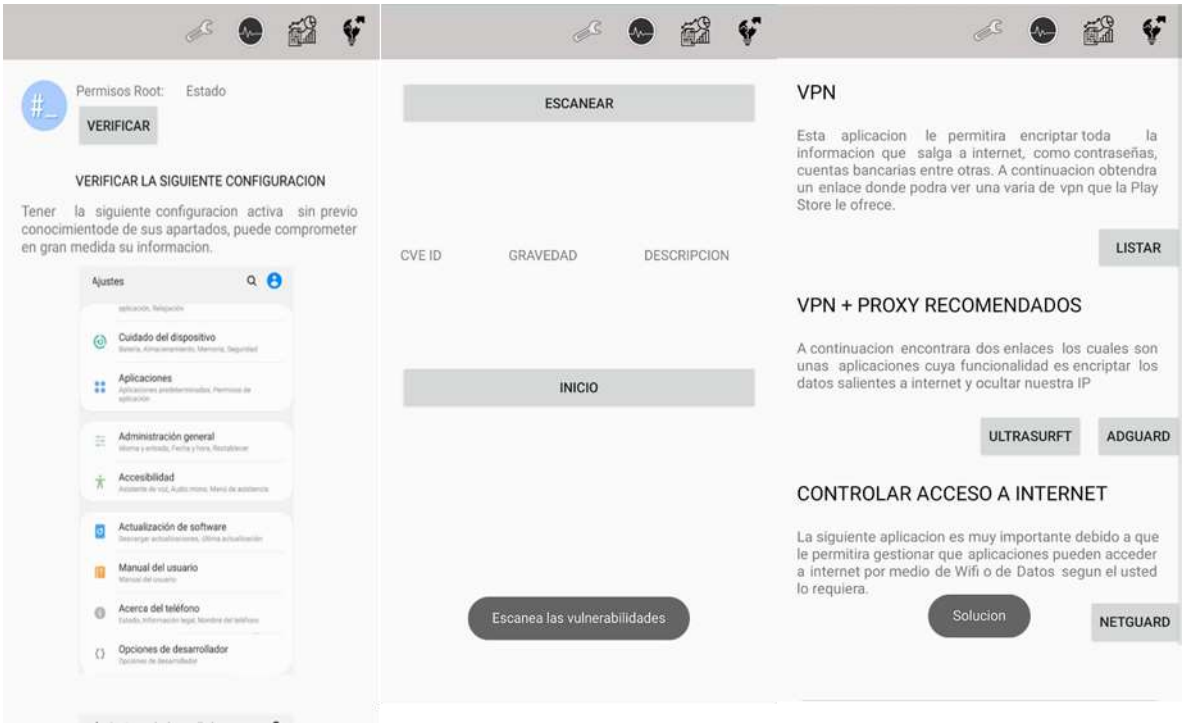

Fig. 4. Modules 1,2,3; Scanner; Root.

Module 3 shows the most frequent attack techniques on mobile devices, it also describes the configurations presented in module 1 and informs why these

configuration options should be disabled (e.g., keep the device without Root access). Moreover, there is a brief description of the module. Finally, Module 4 shows the recommendations of tools and actions that help to take care of the device such as:

- VPN maintains control of the internet connection and modifies the geolocation to make an anonymous bridge of the data managed by the device, on the other hand, it allows to encrypt the susceptible information on the internet.
- VPN + PROXY: This service allows the user to encrypt the outgoing data to the internet and hide the user's IP, using Ultrasurft [13] and Adguard [14].
- CONTROL OF INTERNET ACCESS: Here Netguart is used to control the entry and exit of data to the network, it has a firewall that allows controlling the internet access of each application installed on the mobile device, providing better control of the data flow [15].

III. RESULTS

The evaluation of the case study was conducted with 129 students from different universities in the southwest of Colombia, the installation of the Android Protect application was carried out on the different devices used by the participants, from Android 5.0 Lollipop up to Android 10.0. The scan was successfully performed on those versions and their derivatives. After that, a laboratory where the devices were infected with spyware and persistent backdoor [16] was developed. The practice consisted of verifying the effectiveness of the Android Protect to stop the viruses. Other sections such as Root access detection and configuration enabled in developer mode were also evaluated.

Figures 5 and 6 show that 19% of the devices were detected by Google Play Protect, since it is responsible for blocking the installation of malicious applications on their device. The 12% allowed the installation without any protection, and 70% display a message requesting for permission to install it. The 19% of the devices had Root access, allowing them to view any type of data and to modify it, 81% of the devices did not have Root access.

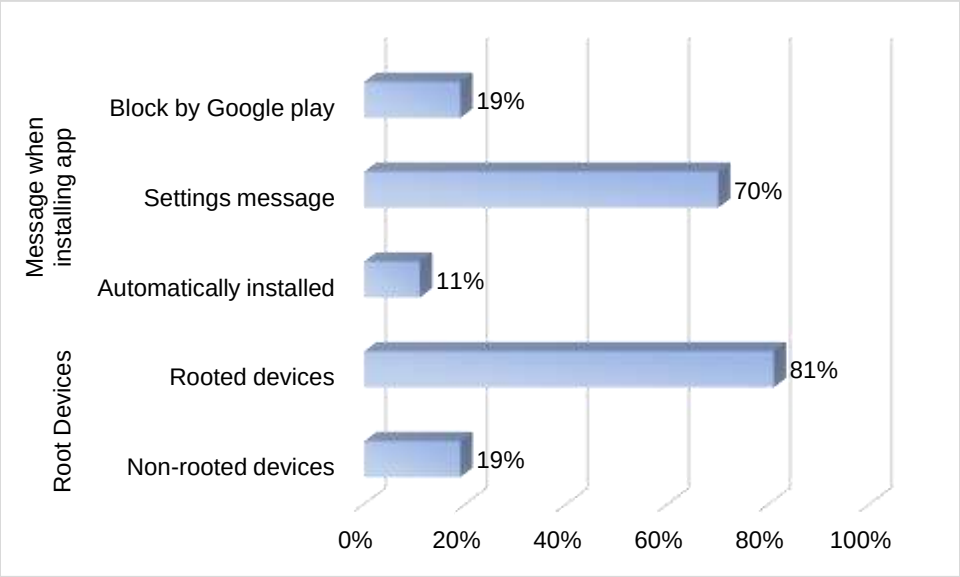

Fig. 5. Results of the case study.

On the other hand, it was observed that 22% of devices had disabled Google Play Protect (The device is pre-configured to accept external applications); 78% have Android protection enabled, so it does not allow applications to be installed automatically. Finally, it is evident that 100% of the devices in the laboratory are vulnerable because none have a stable protection that allows them to prevent the installation of applications or malicious elements.

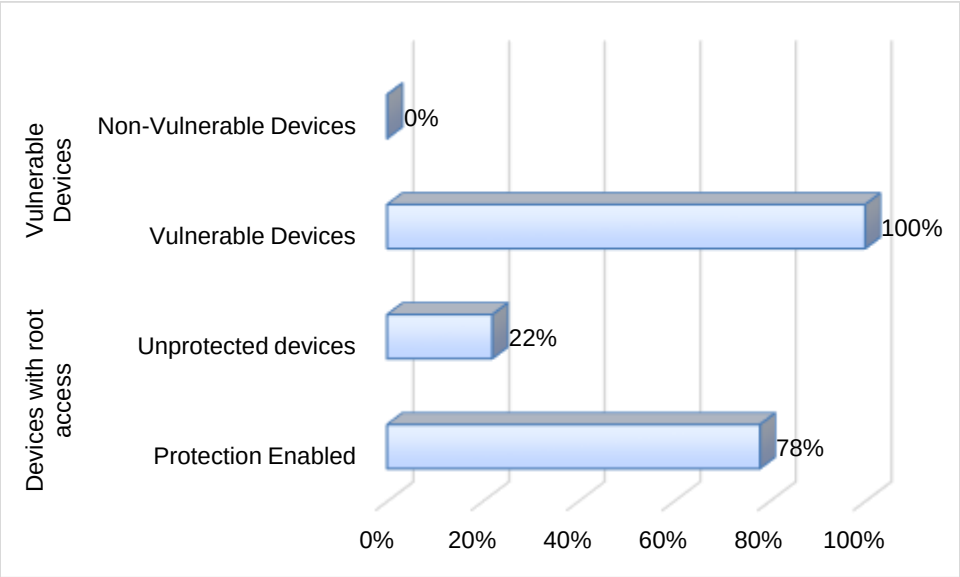

Fig. 6. Results of the case study.

V. Conclusions and Future Work

The case study shows the importance of being aware of security issues in our mobile devices; it is recommended to consider these issues to improve self-care.

A mobile application with four modules was developed to help users to verify the security of the mobile device: First, an analysis of the internal configuration (Root access, debugging mode); Second, scanning vulnerabilities; Third, the most common vulnerabilities are explained; Finally, a section about how to prevent the vulnerabilities.

It is also concluded that 100% of the devices were vulnerable because they had a malicious software blocker; however, it was not enough to prevent malicious installations. Many devices had a wrong permission assigned by the owner; therefore, it is recommended to be informed on the subject and in this way avoid these problems.

Authors' Contribution

Cristian-Camilo Ordoñez-Quintero: Research, exploratory data analysis, model definition and refinement, implementation, model validation.

Hugo-Armando Ordoñez-Eraso: Research, methodology, validation, writing - review and editing.

Jose-Armando Ordoñez-Córdoba: Research, supervision, methodology, validation, writing - review and editing.

Acknowledgment

The authors appreciate the contribution of Fundación Universitaria de Popayán and Universidad del Cauca, where they currently serve as Professors in the Systems Engineering program.

References

[1] N. Valero, *Consumo móvil en Colombia*, Deloitte, 2018

[2] W. C. Álzate, C. S. Romaña, Y. Q. Barco, "Factores y causas de la fuga de información sensibles en el sector empresarial," *Cuaderno Activa*, vol. 7, no. 1, pp. 67-73, 2016

[3] R. Maya, “El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual,” *Nuevo Foro Penal*, vol. 13, pp. 72–112, 2017. https://doi.org/10.17230/nfp.13.88.3

[4] A. C. Silva Calpa, D. G. Martínez Delgado, “Influencia del Smartphone en los procesos de aprendizaje y enseñanza,” *Suma Negocios*, vol. 8, no. 17, pp. 11–18, 2017. https://doi.org/10.1016/j.sumneg.2017.01.001

[5] A. Razgallah, R. Khoury, S. Hallé, K. Khanmohammadi, “A survey of malware detection in Android apps: Recommendations and perspectives for future research,” *Computer Science Review*, vol. 39, e100358, 2021. https://doi.org/10.1016/j.cosrev.2020.100358

[6] H. Gao, S. Cheng, W. Zhang, “GDroid: Android malware detection and classification with graph convolutional network,” *Computers & Security*, vol. 106, e102264, 2021. https://doi.org/10.1016/j.cose.2021.102264

[7] N. Zhang, Y. Tan, C. Yang, Y. Li, “Deep learning feature exploration for Android malware detection,” *Applied Soft Computing*, vol. 102, p. 107069, 2021. https://doi.org/10.1016/j.asoc.2020.107069

[8] M. Kinkead, S. Millar, N. McLaughlin, P. O’Kane, “Towards Explainable CNNs for Android Malware Detection,” *Procedia Computer Science*, vol. 184, pp. 959–965, 2021. https://doi.org/10.1016/j.procs.2021.03.118

[9] Y. Igarashi, “DREBIN: Effective and Explainable Detection of Android Malware in Your Pocket,” *The Journal of Japanese Studies*, vol. 36, no. 1, pp. 165–169, 2009. https://doi.org/10.1353/jjs.0.0130

[10] Y. Wang, G. Xu, X. Liu, W. Mao, C. Si, W. Pedrycz, W. Wang, “Identifying vulnerabilities of SSL/TLS certificate verification in Android apps with static and dynamic analysis,” *Journal of Systems and Software*, vol. 167, e110609, 2020. https://doi.org/10.1016/j.jss.2020.110609

[11] P. Runeson, M. Höst, “Guidelines for conducting and reporting case study research in software engineering,” *Empirical Software Engineering*, vol. 14, no. 2, e131, 2009. https://doi.org/10.1007/s10664-008-9102-8

[12] NIST, *Marco de Ciberseguridad del NIST*, pp. 1–9, 2019

[13] R. Al-quraan, A. Hadi, J. Atoum, M. Al-Zewairi, “Ultrasurf Traffic Classification: Detection and Prevention,” *International Journal of Communications, Network and System Sciences*, vol. 8, pp. 304–311, 2015. https://doi.org/10.4236/ijcns.2015.88030

[14] D. Howe, H. Nissenbaum, *Engineering Privacy and Protest: A Case Study of AdNauseam*, 2017

[15] A. Skendzic, B. Kovačić, “Open source system OpenVPN in a function of Virtual Private Network,” *IOP Conference Series: Materials Science and Engineering*, vol. 200, e12065, 2017. https://doi.org/10.1088/1757-899X/200/1/012065

[16] J. Dai, C. Chen, Y. Li, “A Backdoor Attack Against LSTM-Based Text Classification Systems,” IEEE Access, vol. 7, pp. 138872–138878, 2019. https://doi.org/10.1109/ACCESS.2019.2941376