The 15th International Scientific Conference
eLearning and Software for Education
Bucharest, April 11-12, 2019
10.12753/2066-026X-19-052

Mobile Application and Wi-Fi Network Security for e-Learning Platforms

George SUCIU, Muneeb ANWAR, Cristiana ISTRATE
BEIA Consult International, Str. Peroni 16, Bucharest, Romania
george@beia.ro, ma@beia.ro, cristiana.istrate@beia.ro

***Abstract**: e-Learning embodies the use of electronic data along with information and communication technologies (ICT) in education. An e-Learning platform is a web-based software and represents an important tool for educators to create and manage courses on the web. However, due to the close relation of e-Learning with the Internet, such platforms are cyber-threatened and recent attacks have increasingly targeted platforms vulnerable to cryptojacking, a technique used for mining cryptocurrencies using the computing resources of devices from unsuspecting users. The number of educational web platforms has increased in the last years, and are now widespread in the mobile applications environment to reach a broad audience of users. The use of e-Learning mobile applications (m-Learning) enables employees to enrich their professional knowledge on their terms, whenever they want, by ensuring easy access to the learning material available on cloud platforms using any kind of Internet connection. The problem analyzed in the paper is related to the security of these m-Learning applications when connecting to public Wi-Fi network at a hotel or library, as an example of an unsecured network, while an office network is usually considered as secure. Our goal is to identify and mitigate the risks when users connect to a Wi-Fi public network, and also analyze how vulnerable devices are exposed to cybercriminals, as hackers can intercept communications between mobile devices such as smartphones or tablets using public Wi-Fi hotspots, namely a man-in-the-middle (MitM) attack. Furthermore, we evaluate several open source penetration testing tools which aid to the identification of vulnerabilities and propose proper security solutions for e-Learning platforms in the context of using public Wi-Fi networks.*

***Keywords:** e-Learning, Security; Cyber-threats; Mobile Applications; m-Learning; Crypto jacking.*

I. INTRODUCTION

E-learning platform is web-based software, which is generated to advance tools and plugins for the learning process. With the expanding availability of Internet technologies and computing, distance learning advances to prove its importance and has begun to have the same reputation as traditional learning methods. Therefore, many studies have indicated that e-learning has been developing and is widely used all over the world. [1].

The security of wireless connections has been in question since they first appear. Year after year, new vulnerabilities are found, which is the reason why the integrity of the wireless encryption process has been continuously deteriorated. There are public or private Wi-Fi networks. Public Wi-Fi networks have no security, while the private ones use encryption that is regularly determined using WPA2 passphrases/passwords [2]. These handle distinctive techniques to guarantee (to some degrees) the integrity of the Wi-Fi IP-based communications path. WPA2 has been subjected to attack using tools feasible to hijack and break authentication.

Besides the ever-growing advancements in technology, security threats and uncertainties are on the rise. Cybercriminals are growing advanced with the ways they exploit technology, addressing it challenging to eliminate hazards. Cyber-attacks can be on a technological framework, in the formation of malware and viruses, or on human organization, in the way of social engineering or cyberbullying [3,4]. Newly, some of the fastest-growing associated crime threats have driven away from exploiting

operations or vulnerabilities on information security and preferably have centered on humans, a target examined to be the weakest connection in every enterprise [5, 6].

Mobile learning (M-Learning) is the newest emphasis of ubiquitous possibly anytime, anywhere learning procedure, where it presents a personalized, sufficiently compact platform. M-Learning is used for little periods of learning, being a method of obtaining knowledge in a preferred subject, anywhere, at any time. Nonetheless, it is based on modern forms of content that are combined in such way to bring interest to learners [7].

The paper is structured in chapters. Section II contains examples of previous research concerning WPA2 security. In Section III, there are overviewed Wi-Fi attack types and assessed penetration tools solutions, choosing Kali Linux for further experiments. The Section IV presents the technologies used and how they were combined to generate the attack. The V. Conclusions chapter summarizes the paper and envisions future work.

II. RELATED WORK

In the past recent years, Moodle became an essential tool in the learning process all over the world. As mobile cloud learning can be seen as a combination between cloud computing and mobile learning, Moodle allows the user to utilize the application on their mobile devices even if they have small memory spaces since it is not needed a special software that will load and save documents. In paper [8] are presented the advantages of using this platform. They detail the way Moodle can be hosted in the Cloud. The article uses as an example Azure, a cloud computing service provided by Microsoft and it describes the operation of deployment. Mobile Moodle in the Cloud was implemented at Khalifa University where they used Moodle 2.0. Moreover, a system called Banner that provides information for the students was integrated within the platform. Therefore, they facilitated communication between students and teachers in a suitable environment for learning.

Nowadays, security has become an important aspect that must be taken into consideration as people will always want their data to be protected. The paper [9] presents a study on security issues cloud service delivery model by creating a model which contains an E-learning part among others. This component is used within the system and can be accessed by users using the secured layer that creates an encrypted connection between server and users.

Authors in [10] recommended an e-learning model to deliver better lectures and contents to the students studying in remote areas, and therefore to enhance the quality of learning and interest. They introduced a bilateral system for e-learning. This system comprises of a dedicated educational satellite. The satellite is responsible for distributing the e-learning contents to the universities connected to it. The proposed system [11] is using a satellite that is working on spot beam technology supported with VSAT terminals to improve the performance of e-Learning in remote locations without mobile network coverage. The limitation of the proposed method is the inability to provide a quiz component and attendance in real-time.

The paper [12] explains how social media, mobile, analytics and cloud and Artificial Neural Network (ANN) can be used to build an intelligent e-learning platform. The study uses vLearn as an example to show that data can be received from the cloud. This connection is secured as there were used encryption and decryption techniques. Therefore, hackers will not access any critical data. Moreover, physical security is provided by using a dedicated server which is located at the Institute. However, a couple of disadvantages such as the lack of a feedback system or the inability to check the level of progress associated with each student.

III. WI-FI ATTACKS AND PENETRATION TOOLS ASSESSMENT

Wi-Fi attacks can be used nowadays in many domains, the purpose being not only to access sensitive information, but also to take control of people’s devices.

The types of Wi-Fi attacks that can be used are the following:

- Packet Sniffing: when packet stored data is exchanged within a network. Since wireless networks communicate through the air, it is not difficult to capture the transmitted information. A considerable amount of activity (Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Network Management Protocol (SNMP), and so on) is transmitted in the clear, implying that there is no encryption, the documents being in plaintext for anybody to examine. Therefore, utilizing a solution like Wireshark enables the attacker to retrieve information transfers in plaintext. This can effortlessly conduct to stolen passwords or sensitive information leaks. The encoded information can be retrieved too. However, it's substantially harder for an attacker to decipher these types of packets;
- Man in the Middle (MitM): when an attacker is firstly passively listening to network communication between two parties, then switching to active behavior by modifying the inter-exchanged information. The hacker takes both of the roles participating in the data exchange to steal confidential information, a time during which none of the two are aware of this middleman. The communication participating entities may be two users or a user and an application, while the MitM is revoking the initial connection between them taking each other's place;
- Password Theft: when people log into a website, sending passwords over the network that does not use Transport Layer Security (TLS) or, its older version, Secure Sockets Layer (SSL). But whatsoever, an experienced attacker can get through these encryption methods and retrieve the password in plaintext;
- Jamming: when overflowing an AP with DE authentication frames. This efficiently "floods" the network and avoids passing authentic traffic between entities. No packet capturing is needed by this type of attack, but it can benefit someone by using it against their competitors, like in a business environment, for example. Although, it is such as illegal as the other types of wireless attacks;
- Wardriving: when a hacker drives around searching for vulnerable APs to attack. Nowadays, attackers even use drones to reach APs placed at higher heights;
- Denial of Service (DoS): when a hacker sends a signal, which alters the efficiency of the network or entirely prevents it from operating. Nowadays, it is impossible to protect Wi-Fi networks form this attack entirely, but the 802.11 standards improved the situation by implementing security based on signal selection, that does not allow the same transmissions to be recorded. A novel solution includes a wall and window shades which can prevent a Wi-Fi signal exiting the building. Also, Intrusion Detection Systems (IDS) or Intrusion Prevention Sensors (IPS) for Wi-Fi connections are more successful because they can prevent DoS attacks, or at least, slow down their destructive purpose;
- Distributed Denial of Service (DDoS): when the DoS attack depends on deactivating the system by utilizing all accessible resources. Various devices perform this type of attack at the same time. These devices may be called "zombies" as a remotely operated software controls them without the victim's knowledge;
- Session Hijacking: when an attacker wants to impersonate a user that is accessing a website or a server. This can be achieved because the Internet portals use session IDs, found within cookies, to distinguish between users. Every request after login is sent to the users. Therefore, it is not necessary to find the password but to get the session ID. This can be done with a sniffing tool, to browse within the user's packets and find the desired information;
- WEP/WPA: when people use elder encryption standards. As soon as the attacker gained access to the network, a significant protection layer has been lost. Routers and APs hide the IP address of the Internet using a device with the aid of Network Address Translation (NAT) unless IPv6 is used. This efficiently shadows the private IP address from the people outside their own subnet and prevents them from directly performing an attack, meaning it does not stop them entirely.

Something else to observe is that all smartphones are in danger whenever they make a connection with an open/public Wi-Fi. Regardless of whether utilizing a laptop, tablet or smartphone, accessing an insecure network labels that device for sensitive information extraction. The best solution will be using a Virtual Private Network (VPN).

Referring to penetration solutions tools that exist nowadays, one of them is Kali Linux [13]. Kali represents a Linux distribution, Debian-based, which has a collection of forensics and security instruments. This software includes several functions like vulnerability investigation, web application analysis, forensics, post exploitation, system services, reverse engineering, wireless attacks, information gathering, password attacks and so on. Kali Linux helps recognize vulnerabilities in several applications associated with the network or WWW particularly the cloud computing environment, or any other website developed by trainees or professionals [14].

Another penetration testing tool that can be used is Network Security Toolkit (NST). It provides open-source tools that can detect problems regarding routine security and diagnose networking faults. This distribution can be used as a validation and monitoring tool for servers that host virtual machines written in different languages such as HTML, AJAX, PHP, etc.

BlackArch Linux [15], other distribution, was created to search for security problems that might occur while trying to penetrate a network. It provides more than 1910 tools made created to solve security and forensic issues.

ParrotSec [16] is a Linux distribution that is based on Debian and promises to solve computer security issues. It was made to check problems concerning vulnerability and mitigation or illegal web browsing.

Pentoo [17] is based on Gentoo Linux that provides both installations for 32-bit and 64-bit systems. Moreover, it is also available as an overlay for installation if a Gentoo version is already available. Provides the injection of packets containing wi-fi drivers, as well as multiple tools for penetration testing and security assessment.

After analysing the above mentioned tools we decided to perform a password hacking experiment using Kali Linux, as it is the only one which runs on smartphones.

IV. PASSWORD HACKING USING KALI LINUX - RESULTS

Secure authentication is required to recognize the user who will use the web application and determine its access privileges. This procedure limits the attackers to access another user's account, to inspect private or protected information or to conduct unauthorized operations. In order to access a private Wi-Fi connection, a user must firstly authenticate by providing the password. Nowadays, the worldwide protocol for Wi-Fi connections is WPA2.

WPA2 [18] is a protocol that contains support for Advanced Encryption Standard (AES) encryption mode and possesses a powerful message and authentication integrity checking used for protection of privacy. WPA2 is difficult to hack because it includes an advanced encryption protocol, namely the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) and a powerful algorithm, the AES. Brute force and dictionary attacks are methods of hacking this type of Wi-Fi when the password has an easy or medium strength. Having the password as difficult to guess as possible, containing alphanumeric and special characters, will skyrocket the chances of not being found by these types of attacks.

To find the password of a WPA2, few requirements are needed. The attacker will need a wireless adapter, the free OS Kali Linux and an Access Point (AP) which will be subjected to attack. Kali Linux OS may be installed within a Virtual Machine (VM), on a computer as the default OS, or on a smartphone under the name of Kali NetHunter. The wireless adapter must be recognized and operational and also to be put into promiscuous or monitor mode. After that, traffic capturing can be started, and all APs in range will be visible. After finding the Basic Service Set Identifier (BSSID), which is the AP's Media Access Control (MAC) address, of the chosen device, the hacker will be able to capture packets from that specific SSID and write them to a file. Next, there is only a matter of time until someone connects to the AP and till their MAC address will be subject to spoofing and packet injection. The 4-way handshake will be captured and then added to the same file. The file is run

against aircrack-ng using a wordlist. In the end, aircrack-ng will display the key on the screen. This process is presented (figure 1).

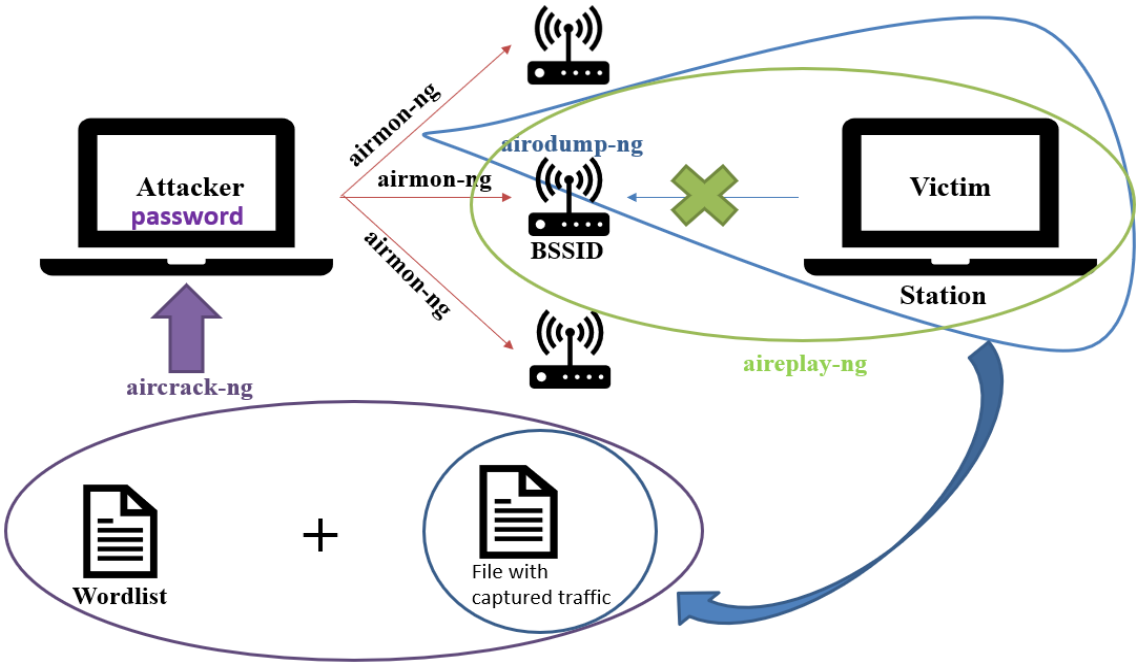

Figure no. 1. Password finding process

Even though WPA2 is the most secure protocol for wireless communication, because all the devices are connected through a wireless interface, a malicious individual will be able to allow or interrupt a connection to an AP. That is, the attacker will decide when the devices will communicate via the Internet with the people in charge of them, which must be avoided.

A script was developed using Kali Linux software suite in order to present the process of finding a Wi-Fi password. In the following lines, some screenshots are displaying the results received by running the script.

General information related to the network connection, like the encryption of the network, the BSSID of the network to be hacked, the Extended Service Set ID (ESSID) of the chosen network and the channel on which the network is listening (figure 2).

```
CH  8 ][ Elapsed: 6 s ][ 2018-06-29 06:11

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

04:F0:21:30:B7:5B  -32       12        0    0  11  130  OPN                 meshliumf958
04:F0:21:2C:74:D8  -45       10        2    0  11  54   WPA  TKIP   PSK  MESHLIUM-AP
00:A0:57:35:29:2C  -48        8        0    0   1  195  WPA2 CCMP   PSK  LANCOMBEIA-LN1702
02:A0:57:35:29:2C  -49        8       72    1   1  195  WPA2 CCMP   PSK  LANCOMBEIA
00:A0:57:30:FA:30  -49        5        8    3  11  130  WPA2 CCMP   PSK  LANCOM_testKALI
02:A0:57:24:57:27  -54       10        0    0   1  195  WPA2 CCMP   PSK  LANCOMBEIA-IT
1A:FE:34:D7:AF:40  -61        6        0    0   9  48   WPA2 CCMP   PSK  uRADMonitor-03
1A:FE:34:D7:AE:D9  -61        7        0    0   9  48   WPA2 CCMP   PSK  uRADMonitor-01
1A:FE:34:D1:80:B2  -63        5        0    0   6  65   WPA2 CCMP   PSK  uRADMonitor-3C
02:A0:57:35:29:F2  -74        0        2    0  10  -1   WPA              <length:  0>
00:A0:57:22:F5:7E  -82        0        4    0   1  -1   WPA              <length:  0>

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   64:5A:04:57:00:BF  -36    0 - 1      2         3
(not associated)   3C:83:75:44:70:08  -90    0 - 1      0         2  LANCOMBEIA
04:F0:21:2C:74:D8  F8:28:19:E2:6A:53  -24   54 -36      0         2
02:A0:57:35:29:2C  DC:85:DE:40:BA:D4  -63    0e- 0e   252        66
00:A0:57:30:FA:30  F8:28:19:C2:53:8F   -1    0e- 0      0         2
02:A0:57:35:29:F2  98:22:EF:2D:F5:7B  -55    0 - 1      0         1

Type the encryption of the network: WPA2
Type the BSSID of the network to be hacked: 00:A0:57:30:FA:30
Type the ESSID of the chosen network: LANCOM_testKALI
Type the channel on which the network is listening: 11
Type the STATION (MAC address) of a client connected to the network: B8:57:D8:24:BE:08
```

Figure no. 2. Information related to the network connection

In the end, after completing the script, the result is being displayed (figure 3).

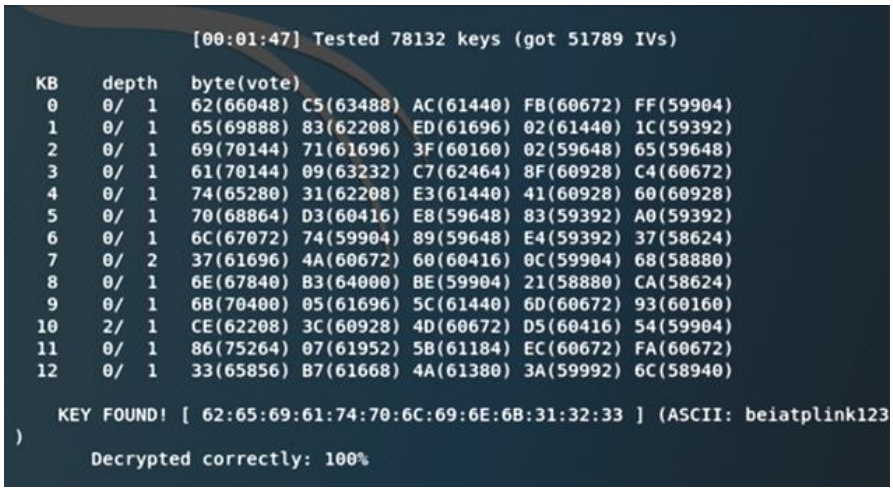

Figure no. 3. The discovered password

V. CONCLUSIONS

This paper analysed the security risk for E-Learning as a method of learning using ICT and electronic devices. E-Learning has been extended to the mobile applications zone (m-Learning) facilitating the learning process especially of employees who want to develop their team's knowledge by using cloud platforms. This paper examined the matter of m-Learning applications security when accessing a Wi-Fi network outside the office's or home place's network, these being considered as secured. Types of Wi-Fi attacks have been presented to show how a hacker may gain access towards the communication between mobile devices that are connected to Wi-Fi. In this paper, there were also assessed various free penetration testing instruments, one of them being Kali Linux which has been used to design a script for finding a WPA2 password and so, allowing the hacker to gain sensitive information on the victim. As future work, a mobile application will be designed to demonstrate this type of attack and mitigation measures.

Acknowledgements

This work has been supported in part by UEFISCDI Romania and MCI through projects ODSI, ToR-SIM and PARFAIT, funded in part by European Union's Horizon 2020 research and innovation program under grant agreement No. 777996 (SealedGRID project) and No. 787002 (SAFECARE project).

References

[1] e-Learning Infographics, 'Top eLearning Stats and Facts For 2015 Infographic - e-Learning Infographics', 2015. [Online]. Available: http://elearninginfographics.com/top-elearning-stats-and-facts-for2015-infographic/. [Accessed: 09- February- 2019]

[2] Gold, Steve; Cracking wireless networks, *Network Security*, no. 11/2011, pp.14-18.

[3] Sarathchandra, Dilshani; Haltinner, Dilshani; Lichtenberg, Nicole; College Students' Cybersecurity Risk Perceptions, Awareness, and Practices, *Cybersecurity Symposium (CYBERSEC)*, IEEE, 2016, pp. 68-73.

[4] Tirumala, Sreenivas Sremath; Hira Sathu; Vijay Naidu; Analysis and prevention of account hijacking based incidents in cloud environment, *International Conference on Information Technology (ICIT)*, Singapore, 2015, pp. 124–129.

[5] Safa, Nader Sohrabi, Rossouw Von Solms, and Steven Furnell, 2016. *Information security policy compliance model in organizations*, Computers & Security, 2016, vol. 56, pp. 70–82.

[6] Tsohou, Aggeliki; Maria Karyda; Spyros Kokolakis; Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs, *Comput. & Security*, 2015, vol. 52, pp. 128–141.

[7] Pandey, Kshama; Neetu Singh; Mobile Learning: Critical Pedagogy to Education for All, *Zhang Y. (eds) Handbook of Mobile Teaching and Learning*, 2015, Springer, Berlin, Heidelberg.

[8] Wang, Minjuan; Yong Chen; and Muhammad Jahanzaib Khan; Mobile cloud learning for higher education: A case study of Moodle in the cloud.
[9] Durairaj, M.; Manimaran, A.; A Study on Security Issues in Cloud based E-Learning, *Indian Journal of Science and Technology 8*, no. 8 /2015, pp. 757-765.
[10] Siddiqui, Ahmad Tasnim; Mehedi Masud; An E-learning system for quality education, *International Journal of Computer Science Issues (IJCSI) 9*, no. 4/2012, p. 375.
[11] Spot Beam Technology. (n.d.). [Accessed: 18- February- 2019] http://www.sadoun.com/Sat/Products/Dishnetwork/Dishes/Spot_Beam_Short.pdf
[12] Mahapatra, Cosmena; Designing a Dynamic E-Learning Platform Using SMAC and ANN, *2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, IEEE, 2015, pp. 941-944.
[13] Hertzog, Raphaël; Jim O'Gorman; Kali Linux Revealed: Mastering the Penetration Testing Distribution, *Kali Linux Revealed: Mastering the Penetration Testing Distribution* 2017, Offsec Press.
[14] Masud, Md Anwar Hossain; Md Rafiqul Islam; Jemal Abawajy; Security Concerns and Remedy in a Cloud Based E-learning System, *International Conference on Security and Privacy in Communication Systems*, 2013, Springer, Cham, pp. 356-366.
[15] Sinha, Sanjib; Setting Up a Penetration Testing and Network Security Lab, *Beginning Ethical Hacking with Kali Linux*, 2018, Apress, Berkeley, CA, pp. 19-40.
[16] Parrot OS webpage: https://www.parrotsec.org/ [Accessed: 18- February- 2019].
[17] Pentoo OS webpage: https://www.pentoo.ch/ [Accessed: 18- February- 2019].
[18] Wahyudi, Erfan; Muhammad Masjun Efendi; Wireless Penetration Testing Method To Analyze WPA2-PSK System Security And Captive Portal, *EXPLORE 9*, no. 1/2019, pp. 1-7.