A Note on a Successful WEP Attack

Stefan Pavlov
Faculty of Computer Science and Engineering
Ss. Cyril and Methodius University, Skopje
stefan.pavlov47@gmail.com

Vesna Dimitrova
Faculty of Computer Science and Engineering
Ss. Cyril and Methodius University, Skopje
vesna.dimitrova@finki.ukim.mk

Abstract

The wireless networks security threats are rising with the development of the wireless technology. The implementation of the security mechanisms in the networks is provided in a way that the mechanisms are incorporated through the wireless network security standards. With the time passing by, there are plenty of efforts in the creation of a multi-layer security system for every wireless network, which would represent the factor of surprise for the attacker, along with the risk of attacks and penetration.

However, unlike other types of data transmission, the wireless data transmission is transmitted in all directions and can be received from any device that is compatible with the wireless adapter. Due to this, it is very important that security mechanisms are implemented so that unauthorized access would be prevented from accessing your network or data.

In order to achieve the best of the security of our data, we need to work for a bigger and deeper implementation of the security measures in every domain of the wireless telecommunication systems. Whether it is about a computer, a mobile or any other sort of device connected to a wireless network, their vulnerability is almost the same, because each and one of them is exposed to a variety of threats and attacks.

That is why the goal of this paper is the research about the attack done on a wireless network.

Keywords—wireless networks, security, privacy, data, threats.

I. INTRODUCTION

The 21th Century is defined by human scientific breakthroughs. One of them is the global use of the Internet. Almost every educated person nowadays knows more or less about the internet. Thereby, a large percentage of the human population make use of the internet on a daily basis. Wireless internet access is thereby made affordable and accessible for everyone and that has boosted human communication and economy development into a new era. However, along with benefits, wireless internet access also possesses several risks and threats of security. The Internet has become a fertile land for criminals of all kinds to operate. Most of all time what they try to take is personal information, some of them extreme values and sensitivity, from naïve and unaware users. In that sense, a comprehensive study on how cybercriminal carry out their attacks and how to avoid and actually prevent such attacks if possible would be beneficial for the righteous netizens. [1]

Devices commonly used for wireless networking include portable computers, desktop computers, hand-held computers, personal digital assistants (PDAs), cellular phones, pen-based, computers, and pagers. Wireless networks work similar to wired networks however, wireless networks must convert information signals into a form suitable for transmission through the air medium.

Wireless networks serve many purposes. In some cases, they are used as cable replacements, while in other cases they are used to provide access to corporate data from remote locations.

Wireless infrastructure can be built for very little cost compared to traditional wired alternatives.

Wireless networks allow remote devices to connect without difficulty, independently these devices are a few feet or several kilometers away. This has made the use of this technology very popular, spreading rapidly. [2]

As we move on, in this section, we will face with two new important issues regarding wireless networks security. The first one of them, is Kali Linux, and the second one, is the process of virtualization.

Kali Linux is an enterprise-ready security auditing Linux distribution based on Debian GNU/Linux. Kali is aimed at security professionals and IT administrators, enabling them to conduct advanced penetration testing, forensic analysis, and security auditing.

The first Kali release happened in March 2013, and was based on Debian 7 “Wheezy”, Debian’s stable distribution at the time. In the first year of deployment, Kali team packed hundreds of pen-testing-related applications and built the infrastructure.

During the first two years following version 1.0, Kali released many incremental updates, expanding the range of available applications and improving hardware support, thanks to newer kernel releases. [3]

As mentioned above, the last part of the introduction is about the process of virtualization. Basically, virtualization is a fundamental part of cloud computing, especially in delivering Infrastructure as a Service (IaaS). Exploring different techniques and architectures of the virtualization helps us understand the basing knowledge of virtualization and the server consolidation in the cloud with different architecture. In this paper we use virtualization as the tool that helps us access Kali without having it installed on a virtual machine. The virtualization tool that we are using here is VMWare. [4]

Then, in Section II, we describe the very basics of wireless networks, and we discuss the main concern of wireless networks – wireless networks security threats.

Afterwards, in Section III, the main focus is set on wireless networks attacks and their classification.

As we move on the next Section IV, the paper gives a brief overview of the latest wireless networks' security standards. Which can be noted as a big deal, due to the fact that, in order to attack, you need to know how to defend at first, and then, you need to know all about standards and policies.

Last but not least, in the last Section V, lies the heart of this paper. In the last section, there is a detailed and deep explanation given on how to conduct an attack on a network using WEP.

II. Wireless Networks Security Threats

Wireless networks are very common, both for organizations and individuals. Many laptop computers have wireless cards pre-installed for the buyer. The ability to enter a network while mobile has great benefits. However, wireless networking has many security issues. Crackers have found wireless networking relatively easy to break into, and even use wireless technology to crack into non-wireless networks. Network administrators must be aware of these risks and stay up to date on any new risks that arise. Also, users of wireless equipment must be aware of these risks, so as to take personal protective measures. Due to this, wireless networks security threats can be classified as home and public.

A. *Home wireless threats*

The need to secure traditional wired internet connections was felt log before. However, there is a growing trend of shifting to wireless connection at home. This involves a process where the user connects a device to his DSL or cable modem that broadcasts the Internet connection through the air over a radio signal to his computer. If traditional wired connections are susceptible to security tribulations, there is a great risk of security breach that may arise when a user opens his Internet connection to the airwaves. An unsecured wireless network coupled with unsecured file sharing can be disastrous. There are, however, steps one can make to protect the wireless network. The following are some of the possible security steps:

- Make the wireless network invisible by disabling identifier broadcasting.
- Rename the wireless network and change the default name.
- Encrypt the network traffic.
- Change administrator's password from the default password. If the wireless network does not have a default password, create one and use it to protect the network.
- Use file sharing with caution. If the user does not need to share directories and files over his network, he could disable file sharing on his computers.
- Keep the access point software patched and up to date.
- Check internet provider's wireless security options as it may provide information about securing your home wireless network.
- Do not auto-connect to open Wi-Fi networks.
- Turn off the network during extended periods of non-use, etc.

B. *Public wireless threats*

The risk to users of wireless technology have increased exponentially as the service has become more popular. There were relatively few dangers when wireless technology was first introduced. Currently, however, there are a great number of security risks associated with wireless technology. Some issues are obvious, and some are not. At a corporate level, it is the responsibility of Information Technology (IT) department to keep up to date with the types of threats and appropriate counter measures to deploy. Security threats are growing in the wireless arena. Crackers have learned that there is much vulnerability in the current wireless protocols, encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level. Cracking methods have become much more sophisticated and innovative with wireless. Cracking has become much easier and more accessible with easy-to-use Windows-based and Linux-based tools being made available on the web at no charge. IT personnel should be somewhat familiar with what these tools can do and how to counteract the cracking that stems from them. Accessing the internet via a public wireless access point involves serious security threats. These threats are compounded by the inability to control the security setup of the wireless network. The following steps can be taken to protect oneself at public places:

- Be careful while dealing in an online environment if the network is not properly secured. Avoid online baking, shopping, entering credit card details, etc.
- Connect using a virtual private network (VPN) as it allows connecting securely. VPNs encrypt connections at the sending and receiving ends and keep out traffic that is not properly encrypted.
- Disable file sharing in public wireless spaces as it is more dangerous than it is on your home wireless network.
- Be aware of your surroundings while using a public wireless access point. If an internet connection is not essential, disable wireless networking altogether. [5]

III. Wireless Networks Attacks Classification

This section contains seven sub chapters that address different attacks against popular wireless protocols and systems. Common themes will emerge throughout it, but each wireless technology has its own unique quirks that make it useful to attackers in different ways, making understanding all of them important to overall security as rarely is just one wireless technology in use at home or office.

A) 802.11 Wireless – Infrastructure Attacks

The ubiquitous 802.11 wireless network is hard to be avoided without running into it. It has become an invaluable resource for both home and office for networking and Internet access. Wireless networking is also incredibly valuable to attackers as it gives the attacker the opportunity to access networks at a safe distance, almost as if they were connected to the wired network. These attacks focus on the infrastructure of these networks and the security implications of their use and how and how not to secure them. They may be ubiquitous, but that doesn't mean they are secure.

A) Wireless – Client Attacks

Wireless clients, those devices that talk to the rest of the wireless network, are mentioned here. Attackers, stymied by increasing amounts of security on the infrastructure side, are changing tactics and attacking client devices directly. At home or away, wireless clients and the information they contain and communicate are tempting targets for pranksters and thieves alike.

B) Bluetooth Attacks

Bluetooth is the subject in these types of attacks. This common protocol was meant to replace cable clutter but has become so much more. While it is meant for short range, any distance can be a comfort for an attacker. Modern devices carry a great deal of information, tempting for a new era of digital pick pockets. You could lose everything without losing anything.

C) RFID Attacks

RFID is a technology most people are not even aware of despite the billions of tags in use every day. As the subject of this type of attacks, RFID is looked at with an eye of how its perceived benefits can actually be their greatest vulnerability and how they can be thwarted by those with ill intentions. RFID is all around us and knowing how to identify it and how to protect it is a very important topic not often understood by many people.

D) Analog Wireless Devices

Even the most modern of wireless devices often at their heart are just radios. Often these new devices are using age-old radio techniques to allow their communication. This type of attack identifies these devices and understands the risks associated with their use and how vulnerabilities apparent over 100 years ago are still around to make life interesting.

E) Bad Encryption

A common solution to wireless security problems is to add encryption. The common problem though with wireless security is bad encryption. Poor design choices, hardware limitations, and cost can all turn a good security idea into a failure at record speed. This problem is being looked over with a number of real-word examples and shows how something that was supposed to protect communications can end up providing less security than advertised.

F) Cell Phones, PDAs, and other hybrid devices

It's impossible to escape them, but cell phones are everywhere. Today's modern smart phones and other hand-held gadgets are at their hard, computers in their own right and have their own unique security issues that need to be considered. In these types of attacks, the main focus is on new generation devices and how their small size, portability and communication capacity make them interesting and tempting targets for today and the future. [6]

IV. Wireless Networks Security Standards

It is important to understand why standards are needed, and the role they play in the adoption and use of technology. The most important reason is for interoperability, enabling multiple vendors to supply equipment that can be integrated into complete systems, ranging from phones plugging into RJ-11 connectors, VCRs connecting to televisions, and in the case of wireless, mobile telephones and wireless modems communicating with wireless networks.

One of the benefits to customers is that an accepted standard reduces technology risk because there are multiple vendors available to choose from. Consumers can change vendors if another vendor offers better prices or features or if a vendor stops supplying equipment. One of the most used standards is known as IEE 802.11b, which has ignited the WLAN industry.

To be successful, there are three questions a standard must address:

1) Is it useful,
2) Is it complete,
3) Is it practical,

In Figure 1 is presented how we can evaluate a standard. [7]

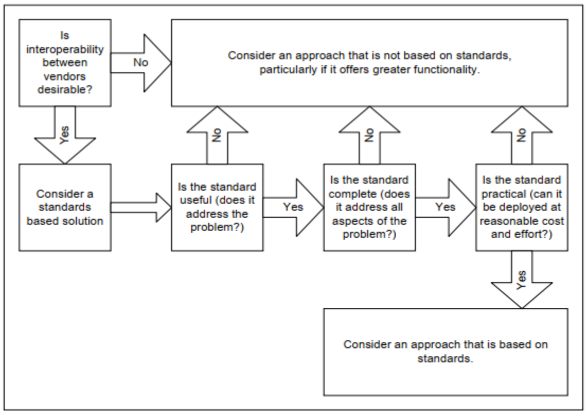
Is interoperability between vendors desirable?
No
Consider an approach that is not based on standards, particularly if it offers greater functionality.
Yes
No
No
No
Consider a standards based solution
Is the standard useful (does it address the problem?)
Yes
Is the standard complete (does it address all aspects of the problem?)
Yes
Is the standard practical (can it be deployed at reasonable cost and effort?)
Yes
Consider an approach that is based on standards.

Fig. 1. *Decision process for standards-based solutions*

When standards do not properly address needs, the marketplace resists adoption. Because Mobile IP does not fully address all of the issues surrounding mobility, key vendors like Microsoft are not supporting the standard. This further erodes motivation for other vendors to support it, and the standard simply has not been able to achieve critical mass.

TABLE I. Merits of different standards

	Strengths	**Weaknesses**
TCP/IP Protocol Suite	Universally accepted. Excellent interoperability.	Not Optimized for wireless connections. No mobility support.
Mobile IP	Provides a mechanism for forwarding packets to a host operating in another network.	Does not address other mobility aspects such as loss of connections or link optimization. Not widely accepted.
IPv6	Increased address space. Mobility Support. Security Mechanisms.	No deployment today. Huge logistics issues for widespread deployment.
IPSec	Security Mechanisms.	No built-in mobility support.

In this Table 1, we can see the merits of the different standards being used in present day. [7]

V. Wired Equivalent Privacy

In the beginning it's believed that WEP offers impenetrable resistance to eavesdroppers/hackers. However, as wireless networks began to grow in popularity, many crypt analysts and researchers discovered flaws in the original WEP design. Many of the WEP flaws would have been caught in the early design phase if it's design and implementation specifications had been reviewed thoroughly. For most of the wireless networking users, WEP is the only choice available until new security mechanisms are added to the IEE 802.11 standard. But as people say "something is better than nothing", even with its known weaknesses, WEP is still more effective than no security at all.

The design objectives of WEP as per section on 8.2.2. of the IEE 802.11 standard states the following:

- "*It's reasonably strong:* The security afforded by the algorithm relies on the difficulty of discovering the secret key through a brute force attack. This in turn is related to the length of the secret key and the frequency of changing keys. WEP allows for the changing of the key (K) and frequent changing of Initialization Vector (IV)."
- "*It is self-synchronizing:* WEP is self-synchronizing for each message. This property is critical for data-link-level encryption algorithm, where "best effort" delivery is assumed, and packet loss rates may be high."
- *"It may be exportable:* Every effort has been made to design the WEP system operation as to maximize the changes of approval, by the U.S. Department of Commerce, of export from the U.S. products containing a WEP implementation. However, due to legal and political climate toward cryptography at the time of publication, no guarantee can be made that any specific IEE 802.11 implementations that use WEP will be exportable from the USA."
- *"It is optional:* The implementation and use of WEP is an IEE 802.11 option."

From the above objectives, it's clear that WEP was not designed to provide a high military level security. The intention was to make it hard to break-in as opposed to impossible to break-in. [8]

VI. Attempting an Attack on WEP

In this section of the paper, we will discuss about how one of the flaws of Wired Equivalent Privacy protocol is being exploited by attackers. As we mentioned above, there are many different attacks that take place on a daily basis everywhere in the areas of IT. By this, we mean either physical or digital attacks occur reaching high numbers. In the example that follows, we will exploit the weaknesses of a wireless network, and the security protocol it uses, WEP.

One of the easiest and the most useful attacks for wireless networks are those that require the least time and effort. One of those types of attacks is a wireless network password cracking attack.

To conduct this type of attack we will be needing:

- Computer (either PC or laptop),
- Additional network card,
- VMWare application installed,
- Kali Linux OS installed on the VMWare virtual machine,
- Kali Linux OS wireless network tool exploiter – Aircrack,
- Network that provides us with Internet access,

- Network that we will be attacking,
- Txt. file that provides us with possible passwords.

The attack occurs as follows:

1) Once we have VMWare installed on our computer, we create a virtual machine, with the dedicated resources needed to run the OS we need for Aircrack – Kali Linux,
2) Then we power up the virtual machine with Kali Linux running on it,
3) When the machine is powered up, we then configure the set-up of the two network cards we provided our computer with. The first one, which is the integrated, provides us with Internet access. While the second one, which is the additional, provides us with the so-called spoofing that shows us which networks are active in the antenna coverage that we have,
4) Afterwards, we move on to launching Aircrack,
5) After Aircrack is launched, a terminal pops-up and we execute the command in the terminal window that provides us with the networks that are broadcasted in our antenna coverage,
6) Since we have all the networks running in our antenna coverage, we choose which network we want to penetrate, and then, we choose which user we want to de-authenticate, by doing this, we are executing two commands, one for network scan, other for user de-authentication selection,
7) When the de-authentication part is done, the user's device automatically tries to reconnect itself to the wireless network access point, and by sending the handshake, which is intercepted by us, it provides us with the information needed to crack the network's password,
8) Last, we need to execute the command that starts the brute force attack, by checking each and every one of the words put in the .txt file,
9) When the password is cracked, we get information details about the network cracking, and the most important part of the cracking – the network password.

Conclusion

The purpose of this paper is to overview the basics of wireless networking technologies, which includes:

- Wireless Network Security,
- Wireless Network Standards, and
- Wireless Network Attacks.

The analysis given in this paper gives a framework fit to describe everything you need to know when conducting an attack on a wireless network or defending one from an attacker. It is fundamental to know how to use wireless networks properly, or securely.

Besides the Wireless Networking Technologies, two more essential points are being monitored here. One is the Kali Linux OS and the other one is VMWare. These two are the key ingredients if you are broke and you cannot provide yourself with a physical machine capable of wireless network penetration, due to the fact that both, Kali Linux and VMWare are free.

To conclude, this paper could prove as a good reference to someone who is new to digital forensics. The topics that this paper provides are the fundamental key elements in getting to know wireless networks and security issues regarding them.

References

[1] Hoa Gia Bao Nguyen, "Wireless Network Security," Lahti University of Applied Sciences, Lahti, Finland, p. 2, 2018.

[2] Jordi Salazar, "Wireless networks," Czech Techical University of Prague, Prague, Czechia, p. 6, 2017.

[3] Raphael Hertzog, Jim O'Gorman and Mati Aharoni, "Kali Linux Revealed: Mastering the Penetration Testing Distribution," Offsec Press, Cornelious, NC, USA, pp.2-3, 2017.

[4] Hyungro Lee, "Virtualization Basics: Understanding Techniques and Fundamentals,", School of Informatics and Computing, Indiana University, Bloomington, IN, USA, p. 1, 2014.

[5] Inyiama H. Chibueze, Achi I. Ifenayi and Agwu O. Chukuemeka, "Threats and security measures on wireless local area networks," Department of Electronic and Computer Engineering, Nnamdi Azikwe University-Awka, Nigeria, p.2, 2014.

[6] Brad Haines, "Seven Deadliest Wireless Technologies Attacks," Syngress, Elsevier, Burlington, MA, USA, pp. 14-16, 2010.

[7] Peter Rysavy, "Networking standards and Wireless Networks,", NetMotion Wireless, Seattle, WA, USA, pp.2-6, 2002.

[8] Shivaputrappa Vibhuti, "IEE 802.11 WEP(Wired Equivalent Privacy) Concepts and Vulnerability," San Jose State University, CA, USA, pp.2-4, 2005.