Control Theory and Informatics
ISSN 2224-5774 (Paper) ISSN 2225-0492 (Online)
Vol.5, No.5, 2015 

# Security Analysis of WPA2

Joseph Mwangi Dr. Wilson Cheruiyot Dr. Michael Kimwel
School of Computing and Information Technology Jomo Kenyatta University of Agriculture and Technology

**Abstract**
Wireless networks provide convenient and low cost mechanism for connecting network devices. They are ideal since they do not require physical connections .They therefore helps overcome the port limitations of the physical hardware. Any device that has radio receiver can detect these wireless signals as the wireless router transmits the signals uniformly in all directions. The ease with which connections can be established exposes wireless networks to many attacks. The authentication protocols have been developed to deter any illicit access to wireless networks, Wi-Fi Protected Access version 2 being one of them. The objective of this research paper was to demonstrate that one can still break the Confidentiality, Integrity and Availability (CIA) triad in the presence of this authentication protocol. The set up was implemented in Ubuntu 12.04 operating system using Ettercap, File2air, Khexedit , Wireshark and Airodump-ng from Aircrack-ng suite. The results indicated that WPA2 does not actually protect data in transit in wireless networks, and therefore there is need to explore other technologies that can secure wireless networks.
**Keywords**:WPA2, CIA Triad, Wireless, Security.

## I. Introduction

The CIA triad consist of Confidentiality, Integrity and Availability (Klingsheim, 2008). By fulfilling these goals, the integrity of the information that is in transit can be assured. Confidentiality deals with protecting the information from disclosure to unauthorized parties. Integrity is concerned with protecting information from being modified by unauthorized parties. Availability is all about ensuring that authorized parties are able to access the information when needed (Terry, 2012).

The two most common encryption schemes for wireless networks include Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). The WEP algorithm is a method of securing wireless internet connections (Blank, 2010). This scheme was developed in 1997 and subsequently becoming the standard for wireless security. However, according to Tews, 2008, the WEP protocol and its underlying cryptographic primitives have been found to be vulnerable on a number of levels. This led to the development of WPA, which is the second encryption standard and it solved most of the problems that were associated with WEP. Hence many security-conscious people, resolved to utilize it on their routers. Unfortunately, WPA uses a password. When a network device connects to the WPA-secured network controller, an encrypted form of this password is transmitted. This encrypted password can easily be held up and put of the air by someone who is listening in (Marshall, 2010). The latest version of WPA is the Wi-Fi Protected Access version 2 (WPA2). According to Bradley, 2010, WPA2 was designed to improve the security of Wi-Fi connections by requiring use of stronger wireless encryption than what WPA requires. Specifically, WPA2 does not allow use of an algorithm called TKIP (Temporal Key Integrity Protocol) that has known security holes. However, this paper sought to demonstrate that this version of WPA has security loop holes.

## II. Methodology

An experimental research was adopted in this paper. This involved setting up one computer as an intruder, another computer as the target and a wireless router as an access point. The experimental set up that was used in shown below.

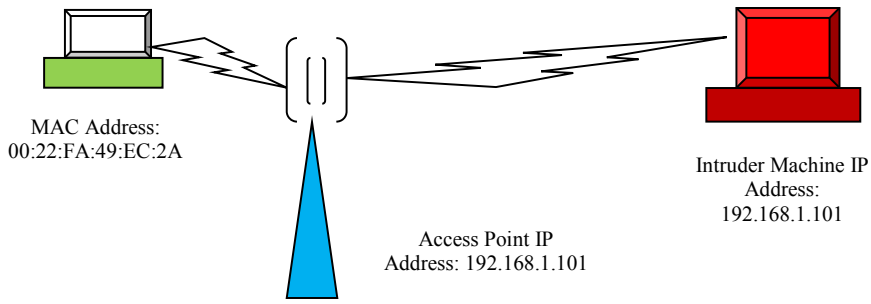


Figure 1: Experimental Setup

**Procedure 1**

1. The target machine was selected. A machine with Media Access Control (MAC) of 00:22:FA:49:EC:2A, as shown above, was chosen.

 

2. The researcher launched a traffic analysis using Airodump-ng from Aircrack-ng suite.
Ettercap, Ubuntu, Airodump-ng from Aircrack-ng suite.
3. The researcher started Address Resolution Protocol (ARP) poisoning attack. This was done by using the following Ettercap command:
*Ettercap –T –M arp:remote –i eth1 /192.168.1.101/*
In the next experiment, the researcher used File2air, Khexedit , Wireshark software and the Ubuntu 12.04 operating system. The setup shown below in Figure 2 was used to bring about deteriorating network performance.

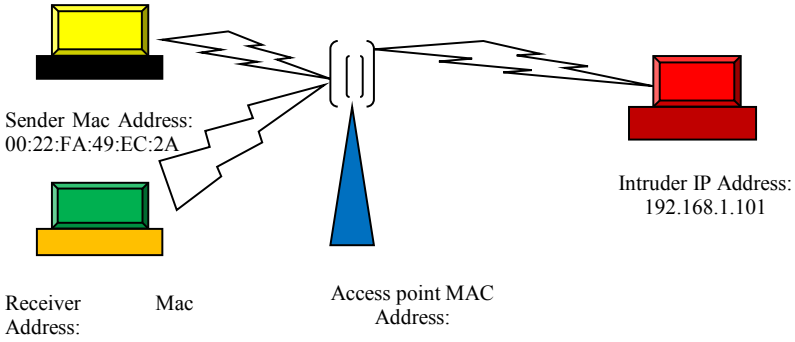


Figure 2: Experimental Setup 2

**Procedure 2**
1. The Khexedit editor was used to generate the fake control frames in the standard format of IEEE 802.11.
2. The fake control frames were continuously transmitted to the target access point with attack cycle of 100 forgery frames per second.

**III Results And Discussion**
The command in procedure 1 was used to re-direct all the traffic from the target machine to the intruder machine with Internet Protocol (IP) address of 192.168.1.101. In so doing, it aided the intruder machine to snoop sensitive information from the target machine as shown in Figure 2 below.

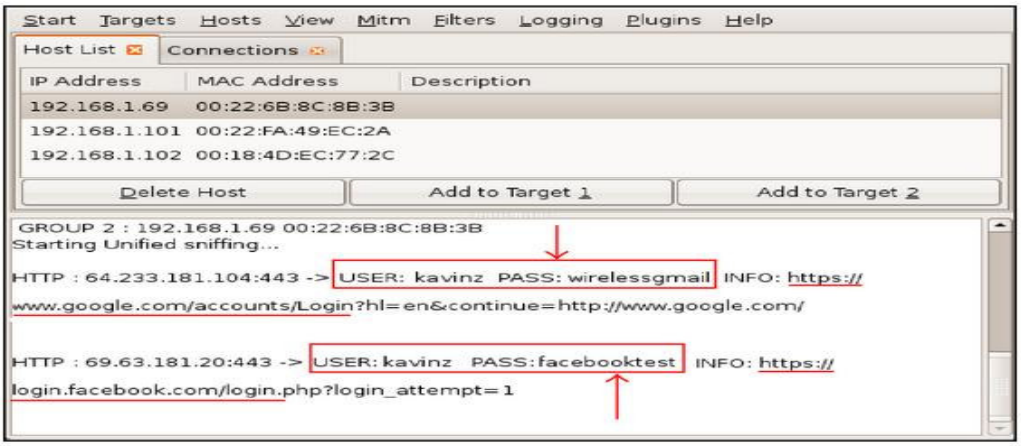


Figure 2: Experimental Output

This Figure shows that the intruder was able to observe the information from the secured Hypertext Transfer Protocol Secure (HTTPS) in the Gmail system. This is because the network traffic has been re-directed to his own machine. In addition, the intruder easily obtained the username (kavinz) and the password (wirelessgmail) of the target user. This user name and password can then be used to gain illicit access to the user account, modify the information hence interfering with the integrity and confidentiality of the user data.

Moreover, the intruder has the opportunity to delete a host from network. If this happens, the users of the deleted machine (Machine with MAC Address of: 00:22:FA:49:EC:2A) would be effectively denied access to the resources that they are entitled to. Obviously, this is a direct attack on the availability of resources.

In relation to procedure 2, the intruder is able to generate fake frames because the frames in transit in wireless networks are stored in little-endian form. This means that proper values in hexadecimal form can be illegally assigned for the Frame Control (FC), duration, receiver MAC address, and transmitter MAC address.

 

Figure 3 below shows the format of the new modified and fake frames.

| | FC | | Duration | | Receiver address | Transmitter address | FCS |
|---|---|---|---|---|---|---|---|
| RTS: | B4 | 00 | FF | 7F | 00:22:6B:8C:8B:3D | 11:11:11:11:11:11 | - |
| CF-End: | E4 | 00 | FF | 7F | 00:22:6B:8C:8B:3D | 11:11:11:11:11:11 | - |
| CF-End-ACK: | F4 | 00 | FF | 7F | 00:22:6B:8C:8B:3D | 11:11:11:11:11:11 | - |

| | FC | | Duration | | Receiver address | FCS |
|---|---|---|---|---|---|---|
| ACK: | D4 | 00 | FF | 7F | 00:22:6B:8C:8B:3D | - |
| CTS: | C4 | 00 | FF | 7F | 00:22:6B:8C:8B:3D | - |

Figure 4: The Generated Fake Frames

It is clear from Figure 4 that the researcher, behaving as an intruder, managed to fix the transmitter address of the forgery control frames to a nonexistent MAC address,. This was done so as to avoid receiving any frame from the target wireless network in response to the forgery frames. The intruder also has fixed the receiver address of the forgery control frames to the target access point. Moreover, the attacker has assigned the maximum possible value in the duration field of the forgery control frames, which is 32767 μs. This was meant to increase the effect of the attacks and to keep the channel reserved as longer as possible. The attacker does not have to calculate the value of the Frame Controls (FCS) for the forgery control frames. This is due to the fact that this value is calculated in hardware by the wireless Network Interface Card (NIC) before sending the frames into the wireless medium. The figure that follows shows the wireless throughput analysis before, during and after fake frame injection.

| Attack | Throughput (Bps) | | | Lost ratio (%) |
|---|---|---|---|---|
| | Before attack | During attack | After attack | |
| ACK DoS-AP | 204972.69 | 0 | 132315.53 | 40 |

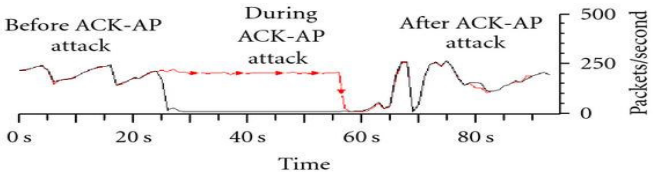


Figure 5: Throughput Analysis

This throughput analysis reveals that the attacks completely rendered the wireless network unusable and made the resources unavailable for the intended users. The fake control frames that belong to the intruder machine (IP-192.168.1.101) have filled the buffer of the access point with illicit worthless information until the access point is not able to respond to the legitimate requests anymore. The large numbers of the fake frames induce a heavy workload to the access point, resulting in wastages of the resources that cannot be recovered for the normal wireless network operations.

**Conclusion**

The researchers managed to achieve the research paper objectives. From the results obtained, it was shown that the CIA triad can easily be broken in the presence of the Wi-Fi Protected Access Version 2 (WPA2) authentication protocol. Moreover, it was demonstrated that network performance can be deteriorated and legitimate network users denied access to the network resources even when WPA2 is implemented, which is supposed to secure wireless networks against these illicit access.

**References**

A. Klingsheim, (2008), *Risks in Networked Computer Systems,* University of Bergen, Norway.
C. Terry (2012), "*Confidentiality, Integrity, Availability: The three components of the CIA Triad*", IT Security Stack Exchange.
Blank , (2010), "*WEP Vulnerabilities and Attacks"*, Research paper.
B. Tews, (2008), "*Practical Attacks Against WEP and WPA"*.
B. Marshall, (2010), "*How WPA Password Cracking Works"*.
M. Bradley *(2010), "WPA2 vs WPA for Wireless Security"*.