Universal Journal of Communications and Network 3(2): 35-40, 2015 http://www.hrpub.org
DOI: 10.13189/ujcn.2015.030201

Practical Attack on Wi-Fi Protected Access Version 2 Authentication Protocol

Vincent N. Omollo[1,*], Ruth K. Chweya[2]

[1]Jomo Kenyatta University of Agriculture and Technology, Kenya
[2]Kisii University, Kenya

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 help to overcome the port limitations of the physical hardware. Any device that has radio receiver can detect these wireless signals. This is because a wireless router transmits the signals uniformly in all directions. The ease with which connections can be established forms one of the weaknesses of wireless networks. They are therefore exposed to many attacks as these attacks can be launched from a remote location, unlike in wired networks where one needs physical connections to the network of interest. To overcome this challenge, authentication protocols have been developed to deter any illicit access to wireless networks. These protocols include Wired Equivalent Privacy(WEP) and Wi-Fi Protected Access (WPA). Wi-Fi Protected Access version 2 (WPA2) is the later version of WPA. The objective of this research paper was to demonstrate that WPA2 can still be broken, hence compromising on the Confidentiality, Integrity and Availability (CIA) of the data being transmitted in wireless networks. Data Confidentiality, Integrity and availability has been referred to as the CIA triad in this paper. 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

1. Introduction

The information being transmitted in the wireless networks need to be protected from unauthorized access. Access Control mechanisms such as passwords, authentication, authorization, and firewalls have been used to deter illegal access to network resources. However, these mechanisms have been shown to be easily compromised. Passwords, for example, can be cracked by using mechanisms such as rainbow attacks and brute forcing. Authentication and authorization can be compromised by masqueraders who can gain access by using other people's credentials. Firewalls can be bypassed by using techniques such as hiding illegal data inside the legitimate data.

The CIA triad consists 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. Sensitive data such as customer credit card numbers should therefore be protected from the spying eyes of intruders.

Integrity is concerned with protecting information from being modified by unauthorized parties. This ensures that the information that clients or workstations are getting is the legitimate data. Hackers have found ways of getting into data on transit re-routing the data to their servers modify the data and re-transmit it back to the network. Therefore, unsuspecting recipient gets corrupted data, hence destroying the reputation of the source of this information. This is common in the business world where competitors want to outdo one another.

Availability is all about ensuring that authorized parties are able to access the information when needed (Terry, 2012).

This means that the downtime should be as little as possible. Downtime refers to the duration which the network resources are inaccessible to the people who need them. In a network environment, downtime can be increased by having redundant route, as the case in mesh networks, so that when one route fails, the other routes can still be used. The RAID (Redundant Array Of Independent Discs) can also be used in servers to ensure that when one hard disc fails, the other hard discs can be utilized.

Encryption is a way of transforming data into some user unreadable format. Hence even if the network data is sniffed, it is in a format that the intruder cannot understand. The sender normally sends the encrypted data to the receiver, who is then supposed to use the required decryption key to decode the message. Without this decryption key, one cannot decode the meaning of the transmitted data.

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 became 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 demonstrated that this version of WPA has security loop holes.

2. Literature Review

The need to protect data and information in wireless networks led to the development of access control protocols such as WEP, WPA, WPA2 and IEEE 802.1X. However, as already stated, these protocols have been shown to have security loopholes. To start with, WEP utilizes the RC4 stream cipher algorithm for authentication and privacy point of view. The challenge with this algorithm is that it was not applied correctly for the WEP technique. RC4 simply performs the XOR operation for the data (Abdul, 2010). Both MAC address and the IV are transmitted in the simple clear text format. Secret keys are shared between network nodes. Data which is encrypted through WEP can easily accessible to attacker through different tools, for example, AirSnort and WEPCrack. Therefore attacks such as brute force attack, attack against key stream re-uses and weak IV(Initialization Vector) attacks (Andrea, 2006).

The main drawback of WPA is that it utilizes Pre-shared Keys (PSKs). This is considered to be a substitute authentication device for small business and home client that do not need to use the individual authentication server and entire 802.1 x key architecture. Moreover, WPA makes use of handshake mechanism to interchange the data encryption keys for the wireless session between the access point and the end user (Habibi, 2009). This is disastrous because an intruder may not know the PSK being used, but can still employ intrusion techniques such as dictionary attack or bruit force attack to guess it.

The main function of using the IEEE 802.1X standard is to provide the port based network access control. According to Abdul (2010), the challenge of the 802.1x protocol is that it circumvents the single authentication procedure over a new process. Moreover, it requires a Remote Authentication Dial-In User Service (RADIUS) server which adds additional costs to its implementations.

The latest version of WPA is the WPA 2. Its main drawbacks are that it is costly to implement for the already deployed networks (Mohammad, 2005). This is due to the fact that it requires a new encryption scheme, known as Counter-Mode/CBC-Mac Protocol (CCMP) and Advanced Encryption Standard (AES). These two protocols require that the overall hardware for the network is altered. Moreover, WPA 2 is fully depended on secrecy session keys, hence the network is prone to attacks.

3. 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.

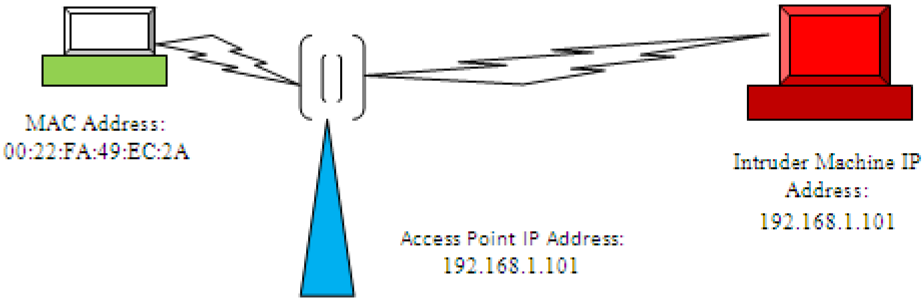


Figure 1. Experimental Setup

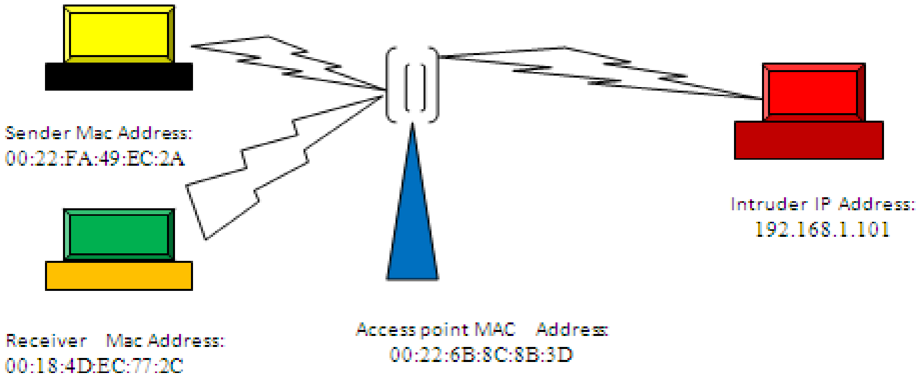
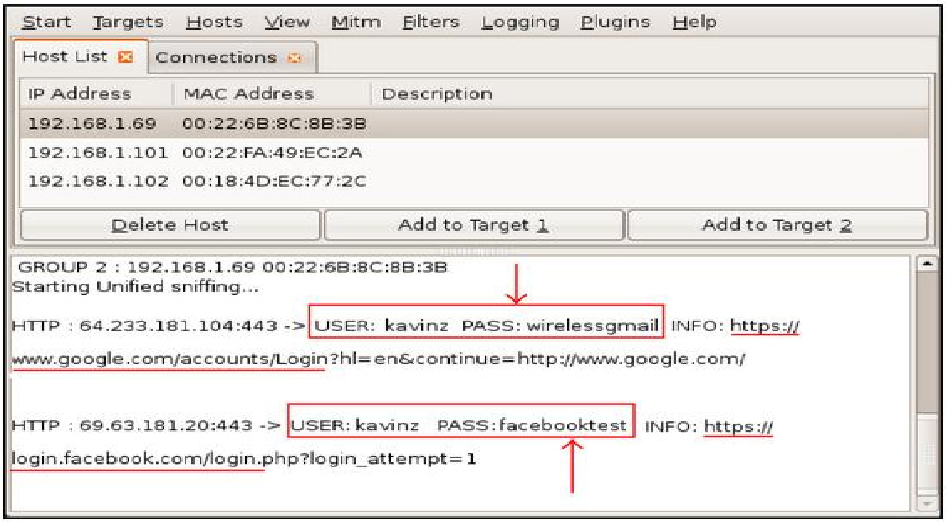


Figure 2. Experimental Setup 2



IP Address	MAC Address	Description
192.168.1.69	00:22:6B:8C:8B:3B	
192.168.1.101	00:22:FA:49:EC:2A	
192.168.1.102	00:18:4D:EC:77:2C	

```
GROUP 2 : 192.168.1.69 00:22:6B:8C:8B:3B
Starting Unified sniffing...

HTTP : 64.233.181.104:443 -> USER: kavinz  PASS: wirelessgmail  INFO: https://
www.google.com/accounts/Login?hl=en&continue=http://www.google.com/


HTTP : 69.63.181.20:443 -> USER: kavinz   PASS: facebooktest  INFO: https://
login.facebook.com/login.php?login_attempt=1
```

Figure 3. Experimental Output

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.

Procedure 2

1. The Khexedit editor was used to generate the fake control frames in the standard format of IEEE 802.11.

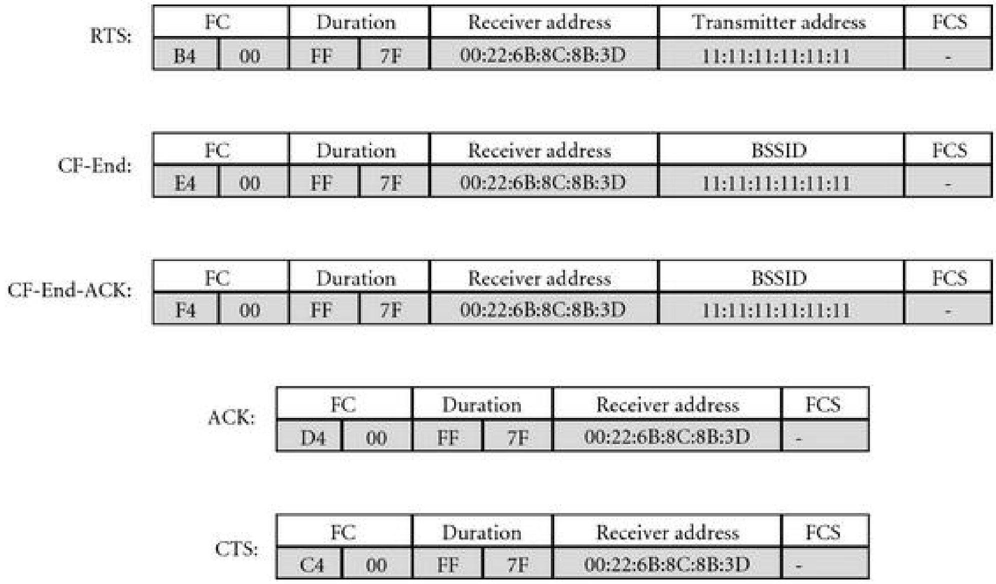
2. The fake control frames were continuously transmitted to the target access point with attack cycle of 100 forgery frames per second.

4. 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 3 below.

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 (wireless mail) 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.



RTS:

FC		Duration		Receiver address	Transmitter address	FCS
B4	00	FF	7F	00:22:6B:8C:8B:3D	11:11:11:11:11:11	-

CF-End:

FC		Duration		Receiver address	BSSID	FCS
E4	00	FF	7F	00:22:6B:8C:8B:3D	11:11:11:11:11:11	-

CF-End-ACK:

FC		Duration		Receiver address	BSSID	FCS
F4	00	FF	7F	00:22:6B:8C:8B:3D	11:11:11:11:11:11	-

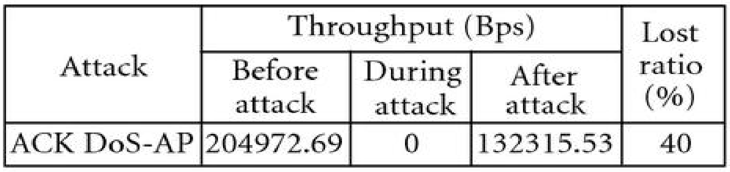
ACK:

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

CTS:

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

Figure 4. The Generated Fake Frames



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

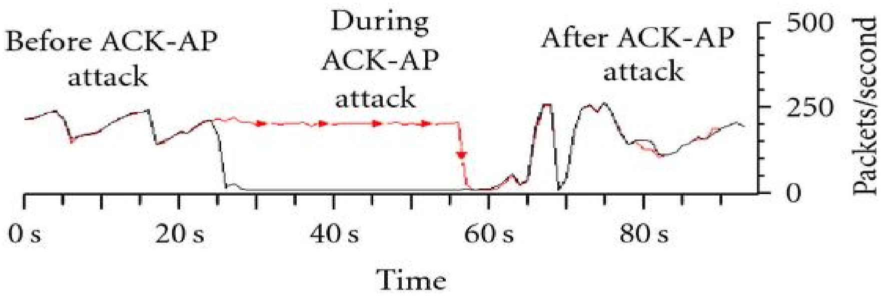
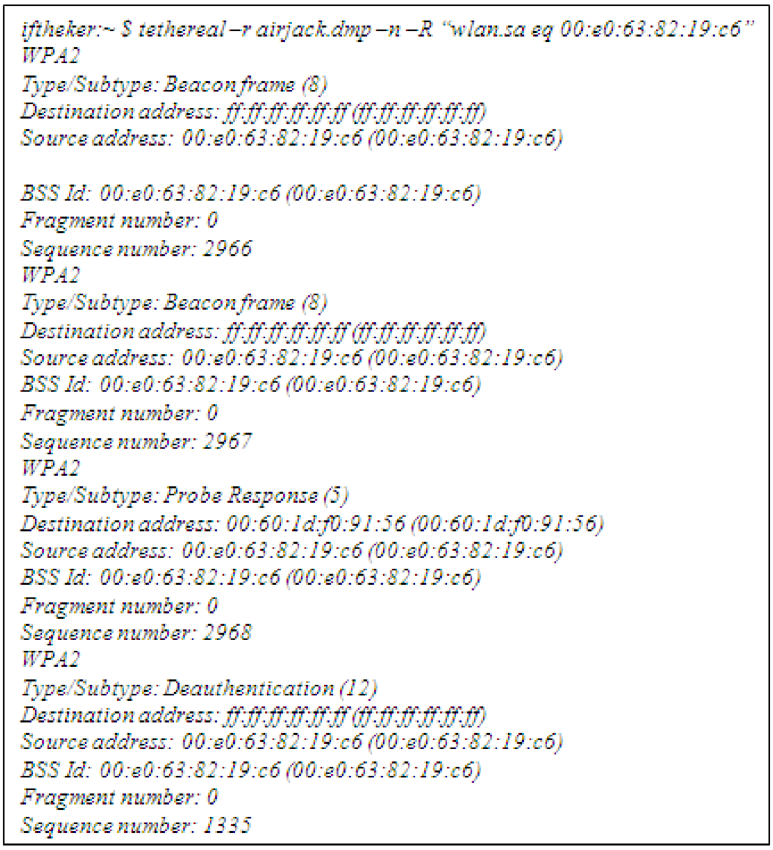


Figure 5. Throughput Analysis

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 4 below shows the format of the new modified and 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.

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.



```
iftheker:~ $ tethereal –r airjack.dmp –n –R “wlan.sa eq 00:e0:63:82:19:c6”
WPA2
Type/Subtype: Beacon frame (8)
Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
Source address:  00:e0:63:82:19:c6 (00:e0:63:82:19:c6)

BSS Id:  00:e0:63:82:19:c6 (00:e0:63:82:19:c6)
Fragment number: 0
Sequence number: 2966
WPA2
Type/Subtype: Beacon frame (8)
Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
Source address:  00:e0:63:82:19:c6 (00:e0:63:82:19:c6)
BSS Id:  00:e0:63:82:19:c6 (00:e0:63:82:19:c6)
Fragment number: 0
Sequence number: 2967
WPA2
Type/Subtype: Probe Response (5)
Destination address: 00:60:1d:f0:91:56 (00:60:1d:f0:91:56)
Source address:  00:e0:63:82:19:c6 (00:e0:63:82:19:c6)
BSS Id:  00:e0:63:82:19:c6 (00:e0:63:82:19:c6)
Fragment number: 0
Sequence number: 2968
WPA2
Type/Subtype: Deauthentication (12)
Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
Source address:  00:e0:63:82:19:c6 (00:e0:63:82:19:c6)
BSS Id:  00:e0:63:82:19:c6 (00:e0:63:82:19:c6)
Fragment number: 0
Sequence number: 1335
```

5. Conclusions and Recommendations

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.

To address the above challenges, the authors propose the utilization of detection tools to determine when frames have been diverted and their content altered. In order to detect irregularity in sequence numbers, there is need to first establish a blueprint of genuine sequence number activity for each MAC address that is to be monitored. For example, let us the machine whose MAC address is “00:e0:63:82:19:c6” to be the legitimate source of the packets in the range of 2966 to 2971. When this pattern is known, we can easily identify the de-authenticate frames as being illegitimate, although they purport to have originated from the source MAC “00:e0:63:82:19:c6”. The AirJack software can be utilized to do this as shown above.

As shown above, the machine with sequence number 1335 is an imposter. This is because its sequence number is well beyond the legitimate sequence number of between 2966 and 2971. Once this, machine has been identified, the network administrator can easily deny access to it. Alternatively, the network administrator can monitor and log its activities so that he can establish the resources that it wants to compromise. This process can yield much meaningful information such as the cracking and hacking tools that the intruder is using to compromise the network and the targeted resources. Thereafter, ways to counter the discovered tools can be devised so as to protect the targeted resources.

REFERENCES

[1] A. Klingsheim, (2008), “Risks in Networked Computer Systems”, University of Bergen, Norway.

[2] C. Terry (2012), “Confidentiality, Integrity, Availability: The three components of the CIA Triad”, IT Security Stack Exchange.

[3] Blank , (2010), “WEP Vulnerabilities and Attacks”, Research paper.

[4] B. Tews, (2008), “Practical Attacks Against WEP and WPA”.

[5] B. Marshall, (2010), “How WPA Password Cracking Works”.

[6] M. Bradley (2010), “WPA2 vs WPA for Wireless Security”.

[7] M. Abdul (2010), “ WLAN Security”, Technical report, IDE1013.

[8] B. Andrea (2006), “The Final Nail in WEP‟s Coffin.”, IEEE Symposium on Security and Privacy, IEEE Computer society.

[9] A. Habibi (2009), “Wired Equivalent Privacy (WEP) versus

Wi-Fi Protected Access (WPA)", International conference on Signal Processing Systems, Singapur.

[10] I. Mohammad (2005), "Hand Book of Wireless Local Area Networks Applications, Technology, Security, and Standard", (internet and communications). CRC Press.