A COMPARITIVE ANALYSIS OF WIRELESS SECURITY PROTOCOLS (WEP and WPA2)

Vipin Poddar
Suresh Gyan Vihar School of Engginering And Technology , Jaipur, Rajasthan
.
Hitesh Choudhary ,
Poornima University , Jaipur, Rajasthan

ABSTRACT

Wireless local area networks (WLANs) are become popular as they are fast, cost effective, flexible and easy to use. There are some challenges of security and for IT administrators the choice of security protocol is a critical issue. The main motive of this paper is to make the non-specialist reader knowledgeable about threats in the wireless security and make them aware about the disadvantages of wireless security protocols. WEP (Wired Equivalent privacy), WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) security protocols are defined and examined here. This security protocols are compared with the common.

This paper is a comparative analysis of WEP, WPA and WPA2. We have tried to perform and check authentication of all 3 protocols by implying the legendary attack vector scripts i.e. Air crack set of tools. The test was conducted on Back Track operating system which is considered as dedicated pentesting operating system. In the test result, we found out that WEP is the weakest, to which WPA was a temporary solution and WPA2 is a very solid and long term solution.

This paper is a mixture of wireless security weaknesses and counter measures to the problems faced until recently. After reading this paper the non specialist reader will have complete review and awareness about the wireless security and vulnerabilities involved with it.

1.INTODUCTION

The way how they transmits data is the major difference between wired and wireless networks. To access to the tarnsmitted data is the main difference between wired and wireless networks. Taping the media that is used in network coomunication is the only possible way in wired networks and in wireless networks communication is done with air media. The radio frequency can access the transmitted data by the equipment that is available for a cheap price in the market readily. For the development of security needs for the development stages of wireless technology and its security needs, according to the experts the security is the major issue. The traditional wired networks are inherely more secure than wireless networks, the transmissions which take place in air with the right equipment can easily intercept those transmissions which are broadcasted in the air. To secure the wireless networks is not a easy task. There are a number of security issues that make securing a WLAN difficult.

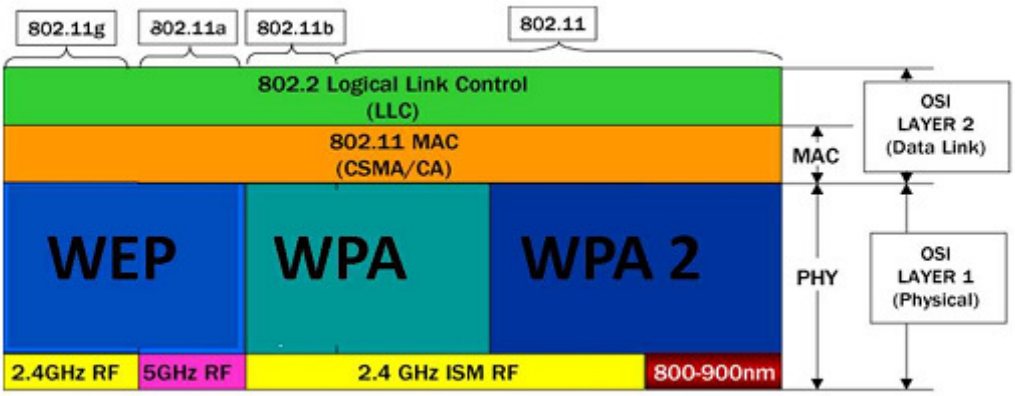
There are three generations of security approaches which are major, which are as follows:

1. WEP(Wired Equivalent Privacy)
2. WPA(Wi-Fi Protected Access)

3. WPA2/802.11i(Wi-Fi Protected Access, Version 2)

DOI : 10.5121/ijans.2014.4301

These protocols are divided as personal and enterprise template.



WIRED EQUIVALENT PRIVACY (WEP)

Wired Equivalent Privacy (WEP)

WEP2 of a volunteer group is an encryption algorithm. The security between two end users of a WLAN is an aim of WEP algorithm over radio signals. RC4 algorithm is used for encryption in WEP and uses two key sizes :40 bit and 104 bit; to which we add a 24- bit initialization vector(IV) which is directly transmitted. The plain text is XOR'ed with the key at the transmitter side, generated after KSA and PRGA process of RC4 and cipher text is obtained. WEp uses CRC-32 algorithm for data integrity.

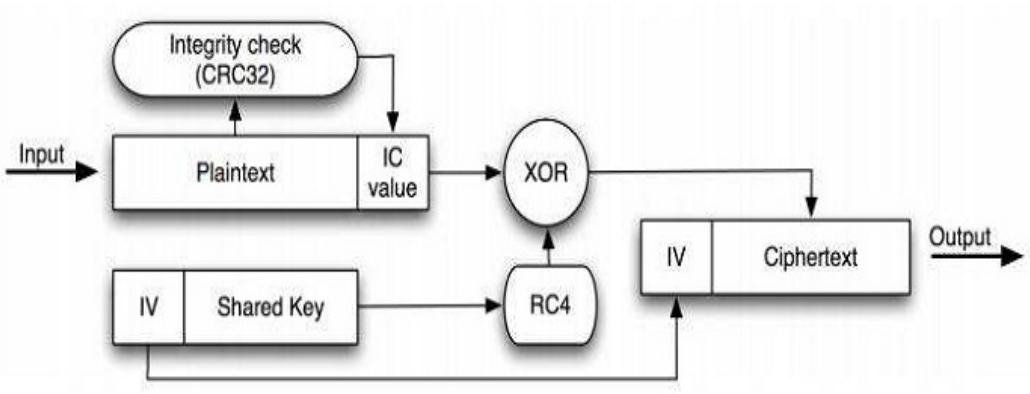


Fig 1. WEP Encryption

WEP Encryption:

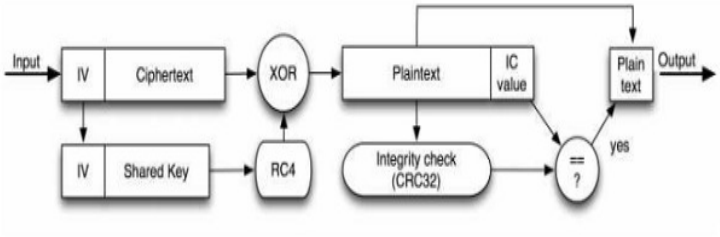


Fig 2. WEP Decryption

Attacking a WEP network

Some flaws in WEP make it crackable. The encrypted packet along with IV is sent as plain text. Thus the information which is out in the air ware can be easily cracked by anyone and can hack the secret key. During few iterations KSA and PRGA leak information of their algorithm. With the help of XOR which is a simple process used to deduce unknown value if the other two values are known. The format is (B+3, 255,x) where B is the byte of the secret key being cracked.

We need lots of IVs in order to sufficiently crack a real life WEP key of a wireless AP. This IVs are not generated very quickly in normal network traffic. It needs lot of patience to crack the WEP key by simply listening of the network traffic and saving them. The process injection is used to speed up the process. Injection involves resending process again and again very rapidly. Thus in a short period of time we can capture a large number of IVs , after determining the IVs we use this IVs to determine the WEP key.

Procedure for Cracking WEP:

STEP 1 wireless card detection.

Figure 1 Detection of wireless card.

Step 2 Network scanning.

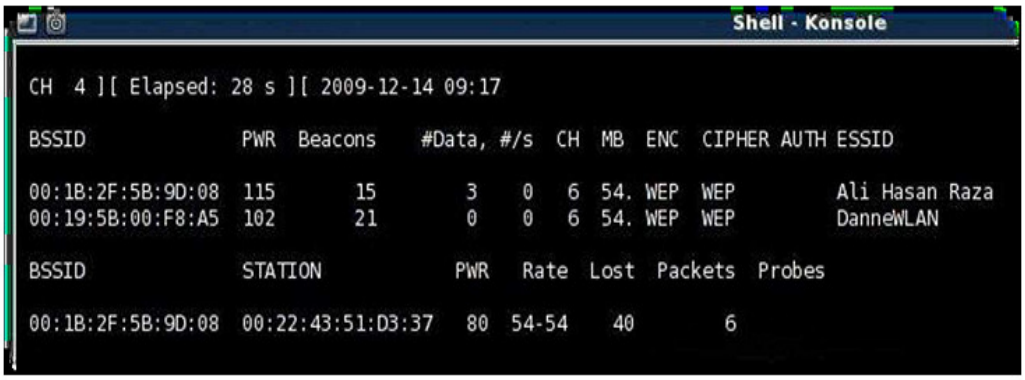


Figure 2. Network scanning

Step 3 Data capturing.

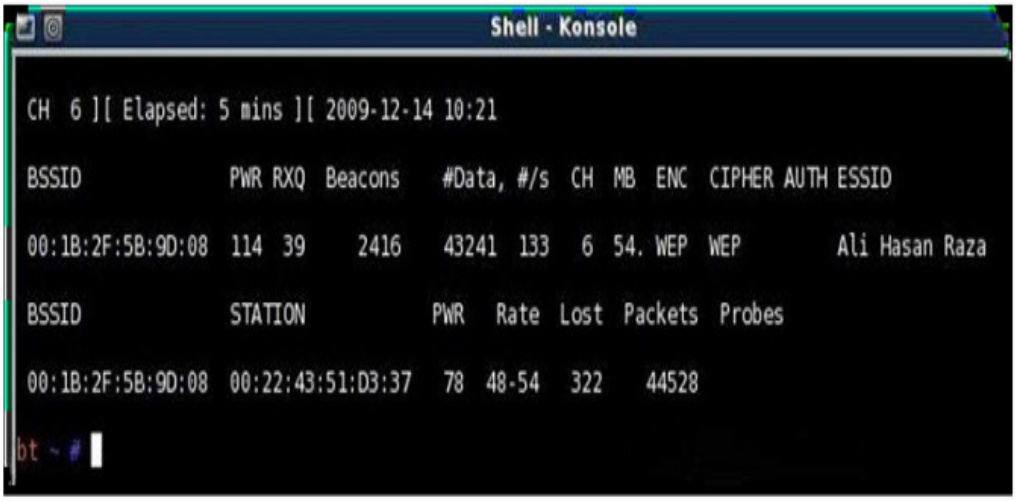


Figure 3. *Data capturing.*

STEP 4 WEP cracking.

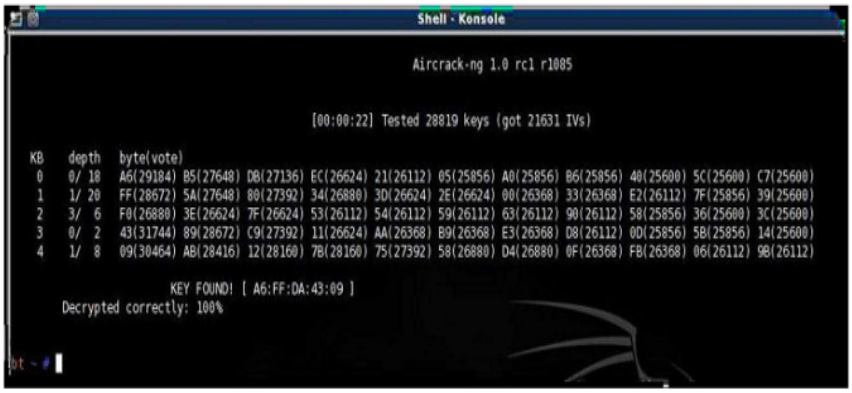


Figure 4 WEP cracking.

Test Results:

Security Mechanism: WEP (40 bit), Time Required: 15-20 min, Mode: Adhoc. Beacon, frames: 10000 IV's captured: 15000, Result: Successful.

WEP Weaknesses:

1. In maintaining a shared WEP key it has disabled a high percentage of wireless networks.
2. WEP has the same problem as the shared key secret is held by another person the private key it becomes public key.
3. The IVs that seeds the WEP algorithm is sent in the secret.
4. The WEP checksum is linear and predictable

Wi-Fi Protected Access (WPA)

To overcome the limitations of WEP the WPA came into existence.WPA is the subset of the IEEE's 802.11i wireless security specification.

Temporal Key Integrity protocol (TKIP) is the encryption method of WPA. The weaknesses of WEP addresses by TKIP by including mixing function, a message integrity check, an extended initialization vector, and a re-keying mechanism. The radius is to authenticate each server, WPA which depends upon central authentication.

The compatible version of IEEE 802.11i is WPA, which is under development. To implement WPA both server and client computers updates their software's during 2003.WEP/WPA modes access points can operate to support both WEP and WPA clients. WEP security level is compatible with mixed level security for all users. The password will trigger authentication and TKIP encryption.

Procedure for Cracking WPA2:

Step 1 Card detection and network scanning:

Step 2: WPA/WPA2 Cracking:

Test Results:

Security Mechanism: WPA2, Mode: Infrastructure, Time Required: 10 min, Attack Type: Dictionary.

Result: Successful

CONCLUSION:

Today the most successful technology that has spread over the world is wireless networks, in order to prevent exploitation of confidential data. In this paper we will focus on three protocols WEP, WPA and WPA2. The overall detailed description of these protocols has been discussed and cracking of these protocols is discussed in this paper. The WPA and WPA2 is not easy to hack as compare to WEP.

REFERENCES:

[1] SANS Institute Reading Room site "The Evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards".
[2] Alexander Gutahr "wired Equivalent Privacy (WEP) Functionality, weak points, Attacks".
[3] Scott Fluhrer, Itsik Martin and Adi Shamir "Weakness in Key Scheduling Algorithm oor RC4".
[4] Bearnard Menezes "network Security and Cryptography.
[5] G. Zepnep Gurkas, A. Halim Zaim, M. Ali Aydin "Security Mechanisms and Their Performance Impacts On wireless Local Area Networks.
[6] http://www.aircrack-ng.org/
[7] Sebastin bohn and Stephan Grob. 2006. An Automated system interoperability test bed for WPA and WPA2 IEEE Xplore
[8] White Paper July 2008. WLAN Security Today: Wireless more secure than wired. Siemens Enterprise Communications.
[9] John S.Park & Derrick Decoy, 2003. WLAN Security: Current and Future, Wireless LAN deployment improves users" mobility, but it also brings a range of security issues that affect emerging standards and related technologies IEEE computer society.
[10] Karen Scafone, Derrick Dicoi Matthew Sexton & Cyrus Tibbs July 2008, Guide to Security Legacy IEEE 802.11 Wireless Networks NIST Special Publication 800-48 Revision 1.
[11] Recommendations Cisco Systems.

About the authors

Hitesh Choudhary:

Mr. Hitesh is an Electronics Engineer working mostly in cyber security domain. In the past he has worked with Indian police department to solve various cyber cases and he is a frequent guest lecturer at many IIT's, NIT's and Texas University.

Vipin Poddar:

Mr. Vipin Poddar is an Electronics engineer and pursuing his master degree. He is currently working deep into the analysis of wireless protocols.