ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I6M9-112012

VOLUME 2 ISSUE 6 November 2012

COMPARISON OF WIRELESS SECURITY PROTOCOLS (WEP AND WPA2)

Disha

Baba Banda Singh Bahadur Engineering College

Fatehgarh Sahib, Punjab

Sukhwinder Sharma

Baba Banda Singh Bahadur Engineering College

Fatehgarh Sahib, Punjab

ABSTRACT

Wireless Local Area Networks (WLANs) are gaining popularity as they are fast, cost effective, flexible and easy to use. They are, however, faced with some serious security challenges and the choice of security protocol is a critical issue for IT administrators. The goal of this paper is to make the non-specialist reader aware of the disadvantages and threats of the wireless security protocols. WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) security protocols are examined in this respect. Then they are compared via

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I6M9-112012
VOLUME 2 ISSUE 6 November 2012

the common features in order to give some insight to those who work with WLANs. We hope this paper give boost to the IT security staff and clarify the common questions of the non specialist reader. More over Wireless networks require very tight security so that the unauthorized users cannot exploit the information. As it is convenient for the hackers to catch wireless signals which spread in the air. Security protocols must be building in order to secure the wireless signals like WPA. The paper discusses the security weakness of Wired Equivalent Privacy (WEP) and provides with the interim and ultimate solutions: Wi-Fi Protected Access (WPA) and 802.11i standards. The paper begins with an introduction of WEP's well-known vulnerability. Many sophisticated authentication and encryption techniques have been embedded into WPA but it is still facing a lot of challenging situations. In this paper we discuss the vulnerability & weakness of WPA. This paper also present solutions or suggestions which will improve Wi-Fi Protected Access (WPA) protocol.

This paper is a compilation of the wireless security weaknesses and counter measures that are put forward until recently. We believe that a thorough understanding of this paper makes the non-specialist reader have a complete review of wireless security and vulnerabilities associated with it.

INTRODUCTION

The major difference between wired and wireless networks is the way that how they transmit data. As for the security risks, the main difference between wired and wireless networks is how to access to the transmitted data. In wired networks this is only possible by tapping the media that is used for the network communication. In wireless networks the media used for communication is air. The transmitted data via the radio frequency can be accessed by

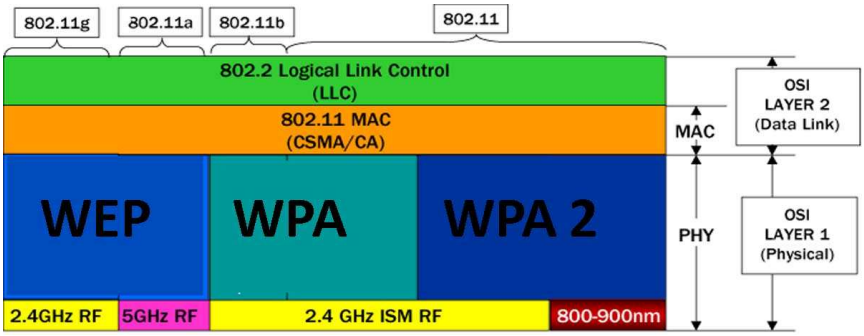
ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I6M9-112012
VOLUME 2 ISSUE 6 November 2012

equipment that is readily available in the market for a cheap price. From the initial development stages of wireless technology and its security needs, experts knew that security would be the major issue. Wireless Networks are inherently less secure than traditional wired networks, since they broadcast information into the air and anyone within the range of and with the right equipment can easily intercept those transmissions. It is for sure that matching all security needs of a wireless network is not an easy task. There are a number of security issues that make Securing a WLAN difficult.

There have been three major generations of security approaches, which is mentioned below:

- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fi Protected Access)
- WPA2/802.11i (Wi-Fi Protection Access, Version 2)

Each of these protocols has two generations named as personal and enterprise template.



WIRED EQUIVALENT PRIVACY (WEP)

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I6M9-112012
VOLUME 2 ISSUE 6 November 2012

The WEP was designed to provide the security of a wired LAN by encryption through use of the RC4 algorithm with two side of a data communication.

Wired Equivalent Privacy (WEP).

WEP [2] is an encryption algorithm developed by an IEEE volunteer group. The aim of WEP algorithm is to provide a secure communication over radio signals between two end users of a WLAN. WEP employs RC4 algorithm for encryption and uses two key sizes: 40 bit and 104 bit; to each is added a 24-bit initialization vector (IV) which is transmitted directly. At the transmitter side the plaintext is XOR'ed with the key stream, generated after KSA and PRGA process of RC4 and cipher text is obtained. These steps take place in the reverse order at the receiver side using the same key. WEP uses CRC-32 algorithm for data integrity.

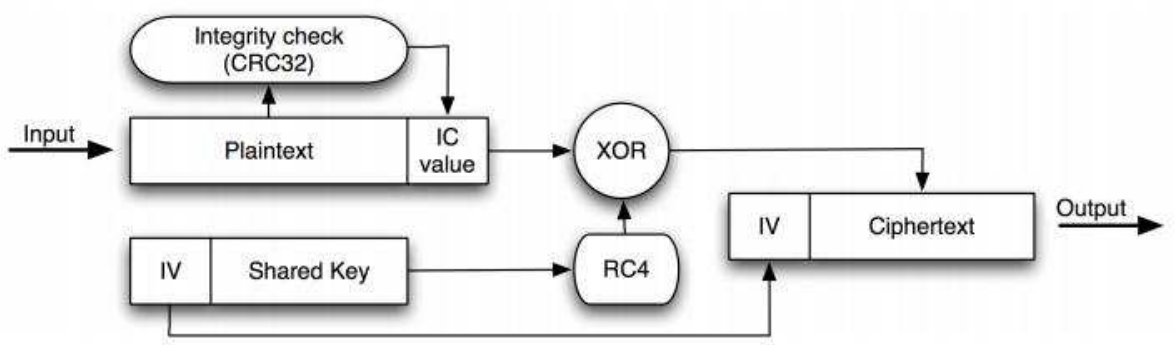


Fig 1. WEP Encryption

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I6M9-112012
VOLUME 2 ISSUE 6 November 2012

WEP Encryption:

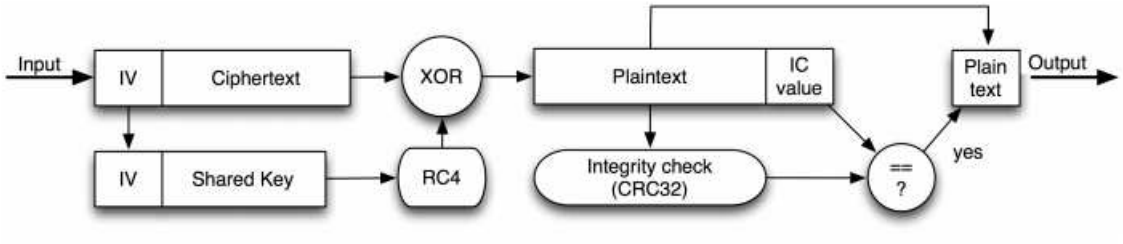


Fig 2. WEP Decryption

There have been problems with WEP due to many security issues. In the 802.11 standard, WEP is defined as "protecting authorized users of a WLAN from casual eavesdropping." As such, WEP is not a terribly strong form of protection and is subject to numerous exploits based on vulnerabilities and weaknesses.

Attacking a WEP network

Some flaws in WEP make it crackable. The IV is sent as plaintext with the encrypted packet. Therefore, anyone can easily sniff this information out of the airwave and thus learn the first three characters or the secret key. Both the KSA and PRGA leak information during the first few iterations of their algorithm. XOR is a simple process that can be easily used to deduce any 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.

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I6M9-112012
VOLUME 2 ISSUE 6 November 2012

In order to sufficiently crack a real-life WEP key of a wireless AP, we need to gather lots of initialization vectors (IVs). Normal network traffic does not typically generate these IVs very quickly. Theoretically, if you are patient, you can gather sufficient IVs to crack the WEP key by simply listening to the network traffic and saving them. However, in this work, we use a technique called *injection* to speed up the process. Injection involves having the AP resend selected packets over and over again very rapidly. This allows us to capture a large number of IVs in a short period of time. Once we have captured a large number of IVs, we can use them to determine the WEP key. In practice WEP cracking can easily be demonstrated using tools such as Aircrack.

Procedure for Cracking WEP:

STEP 1 wireless card detection.

Figure 1 Detection of wireless card.

Step 2 Network scanning.

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I6M9-112012
VOLUME 2 ISSUE 6 November 2012

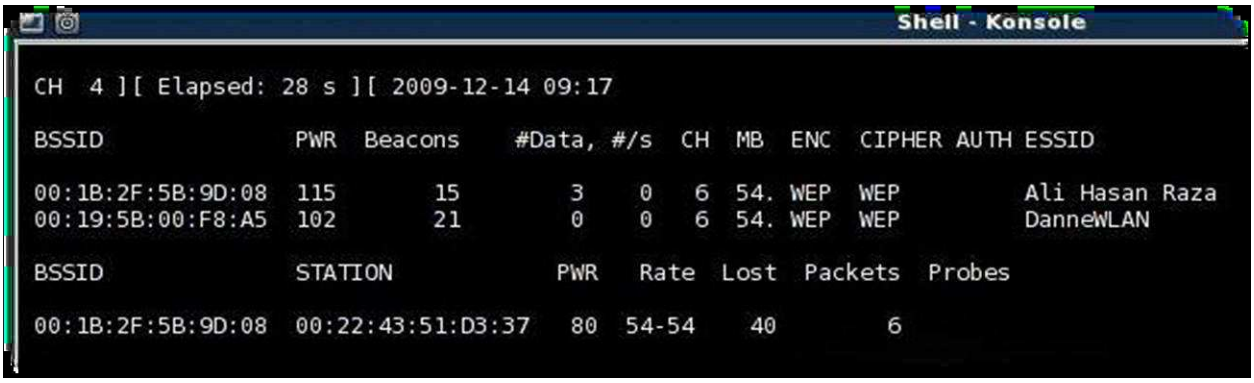


Figure 2. Network scanning

Step 3 Data capturing.

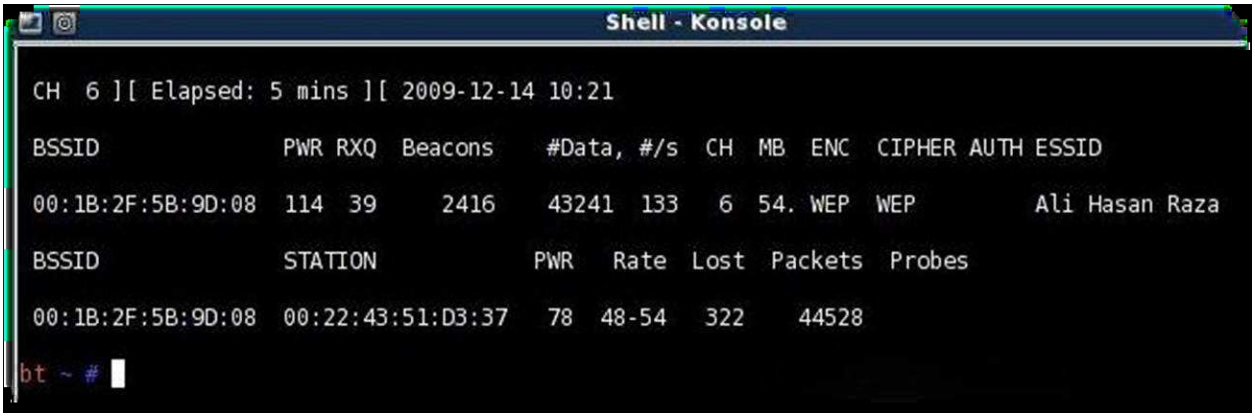


Figure 3. *Data capturing.*

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I6M9-112012
VOLUME 2 ISSUE 6 November 2012

STEP 4 WEP cracking.

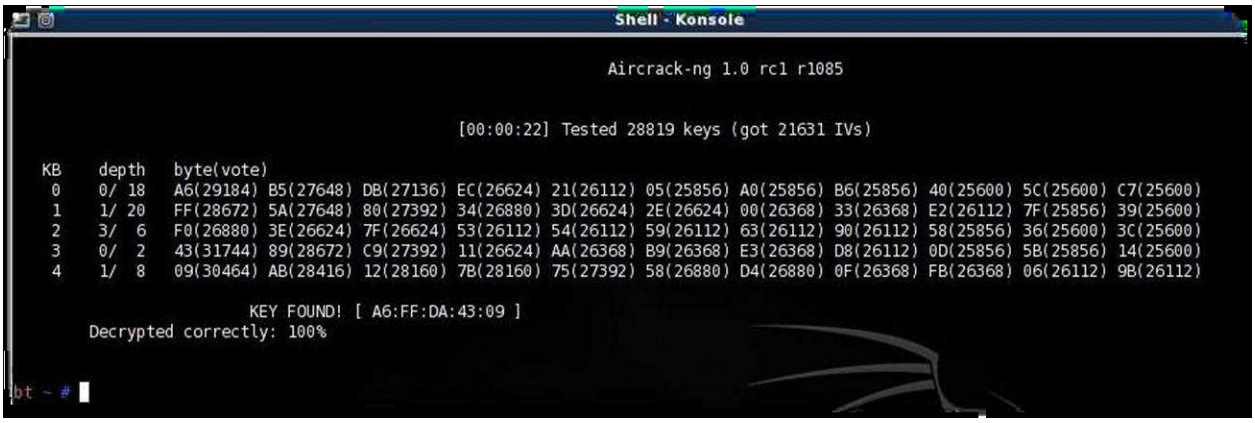


Figure 4 WEP cracking.

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. A high percentage of wireless networks have WEP disabled because of the administrative overhead of maintaining a shared WEP key.

2. WEP has the same problem as all systems based upon shared keys: any secret held by more than one person soon becomes public knowledge. An example is an employee who leaves a company ... the employee still knows the shared WEP key and could sit outside the company

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I6M9-112012
VOLUME 2 ISSUE 6 November 2012

sniffing network traffic or even attacking the internal network.

3. The initialization vector that seeds the WEP algorithm is sent in the clear.

4. The WEP checksum is linear and predictable.

Wi-Fi Protected Access (WPA)

It is an effort to overcome the security limitations of WEP. WPA is subset of the IEEE's 802.11i wireless security specification.

WPA's encryption method is the Temporal Key Integrity Protocol (TKIP). TKIP addresses the weaknesses of WEP by including a per-packet mixing function, a message integrity check, an extended initialization vector, and a re-keying mechanism. WPA provides "strong" user authentication based on 802.1 xs and the Extensible Authentication Protocol (EAP). WPA depends on a central authentication server such as RADIUS to authenticate each user.

Wi-Fi Protected Access is a subset of and will be compatible with IEEE 802.11i (sometimes referred to as WPA2), a security standard under development. Software updates that will allow both server and client computers to implement WPA are expected to become widely available during 2003. Access points (see hot spots) can operate in mixed WEP/WPA mode to support

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I6M9-112012
VOLUME 2 ISSUE 6 November 2012

both WEP and WPA clients. However, mixed mode effectively provides only WEP-level security for all users. Home users of access points that use only WPA can operate in a special home-mode in which the user need only enter a password to be connected to the access point. The password will trigger authentication and TKIP encryption.

Procedure for Cracking WPA2:

Step 1 Card detection and network scanning:

Step 2: WPA/WPA2 Cracking:

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I6M9-112012
VOLUME 2 ISSUE 6 November 2012

Test Results:

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

Result: Successful

CONCLUSION

Wireless networks are becoming the most rapidly spread technology over the world; thus, they should be well protected, in order to prevent exploitation of confidential data. In this paper we presented a brief overview of them, focusing on three main security protocols WEP, WPA and WPA2. We discussed and presented the overall detail procedure for cracking WEP and WPA2. Our motivation was the need for increased wireless security and the common feel that nowadays WPA/WPA2 security protocols are difficult for a stranger to hack; however, our study

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I6M9-112012
VOLUME 2 ISSUE 6 November 2012

depicted that any wireless network may be suffering from successful hacking attempts, if it is not carefully setup and protected.

V. REFERENCES:

- SANS Institute Reading Room site “The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards”.
- Alexander Gutjahr “Wired Equivalent Privacy (WEP) Functionality, Weak Points, Attacks”.
- Scott Fluhrer, Itsik Mantin and Adi Shamir “Weakness in Key Scheduling Algorithm Of RC4”.
- Bernard Menezes “Network Security and Cryptography”.
- G. Zeynep Gurkas, A. Halim Zaim, M. Ali Aydin “Security Mechanisms And Their Performance Impacts On Wireless Local Area Networks”.
- http://www.aircrack-ng.org/
- Sebastin Bohn & Stephan Grob. 2006. An automated system interoperability test bed for WPA and WPA2. IEEE Xplore
- White paper. July 2008. WLAN Security Today: Wireless more secure than wired. Siemens Enterprise Communications.
- Joon S.Park & Derrick Dicoi. 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.
- Karen Scarfone, Derrick Dicoi, Matthew Sexton & Cyrus Tibbs. July 2008. Guide to Securing Legacy IEEE 802.11 Wireless Networks. NIST Special Publication 800-48 Revision 1.

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I6M9-112012
VOLUME 2 ISSUE 6 November 2012

- Anthon James. 2002. Using IEEE 802.1x to Enhance Network Security. Foundary Networks.

- Andrea Bittau, Mark Handley &Joshua Lackey. 2006. The Final Nail in WEP‟s Coffin. IEEE Symposium on Security and Privacy, IEEE Computer society. Martin Beck. 8 November2008. Practical attacks against WEP and WPA. IEEE computer Society.
- Jin Hong & Palash Sarkar. 2005. “Rediscovery of Time Memory Tradeoffs”.
- David A. McGrew. November2002. “Counter Mode Security: Analysis and Recommendations”, Cisco Systems.
- Prasad, N. R., and A. R. Prasad (eds.), WLAN Systems and Wireless IP for Next Generation Communications, Norwood, MA: Artech House, January 2002.
- Black, U., Internet Security Protocols: Protecting IP Traffic, Upper Saddle River, NJ: Prentice Hall, 2000.