IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)
ISSN(E): 2321-8843; ISSN(P): 2347-4599
Vol. 3, Issue 5, May 2015, 23-30

WI-FI SECURITY: A LITERATURE REVIEW OF SECURITY IN WIRELESS NETWORK

RUCHIR BHATNAGAR & VINEET KUMAR BIRLA

Research Scholar & Department of CSE & Mewar University, Chittorgarh, Rajasthan, India

ABSTRACT

As we know wireless networks have broadcast nature so there are different security issues in the wireless communication. The security conventions intended for the wired systems can't be extrapolated to wireless systems. Hackers and intruders can make utilization of the loopholes of the wireless communication. In this paper we will mull over the different remote security dangers to wireless systems and conventions at present accessible like Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2). WPA2 is more hearty security convention as compared with WPA on the grounds that it utilizes the Advanced Encryption Standard (AES) encryption. There are few issues in WPA2 like it is helpless against brute force attack and MIC bits could be utilized by programmer to compare it with the decoded content. So in this paper we will concentrate on different sorts of wireless security dangers.

KEYWORDS: Wi-Fi, Security, WPS, Brute Force Attack

INTRODUCTION

Wireless LAN technology has rapidly become very popular all over the world. The wireless local area network (WLAN) protocol, IEEE 802.11, and associated technologies enable secure access to a network infrastructure. Until the development of WLAN, the network client needed to be physically connected to the network by using some kind of wiring. With the rapid increase in use of WLAN technology it is important to provide a secure communication over wireless network. Since its creation the security of wireless networks went through different stages of development, from MAC address filtering or WEP to WPA/WPA2.The wireless technology was proven to be very practical (not only) for home users. Such a handy option to be comfortably connected to internet on a mobile device without the need of wires is still gaining in popularity. This led to an attempt to make a configuration of WLAN easier for regular user without any knowledge about computer science. The result of this was standard known as Wifi Protected Setup (WPS).WPS, as a standardized technology, is implemented on wide variety of currently produced wireless access points. The incorrect designing of its standard led to fatal weakness which is discussed in this thesis in greater details.

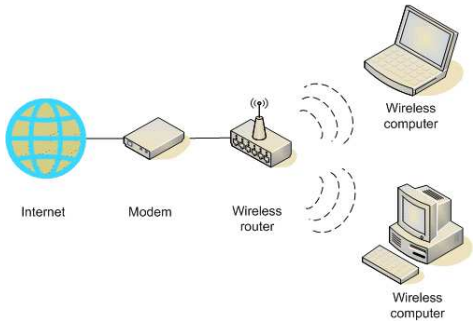

Figure 1: Wireless Communication

The 802.11 networks consist of four major components:

- **DISTRIBUTION SYSTEM** - a logical component used to forward frames to their destination.
- **ACESS OINTS (APs)** - devices performing wireless-to-wired bridging function.
- **STATIONS (STAs)** - device with wireless network interface communicating with other similar devices via APs.
- **WIRELESS MEDIUM** - medium used to transfer frames from station to station.

Weakest Security Mechanisms

Among the most commonly used security mechanisms to protect WLAN while them being no obstruction at all for an even unexperienced attacker are SSID hiding and

MAC ADRESS FILTERING: Many APs offer user an option to hide the SSID. If it is enabled, the AP in its beacon frames does not show the SSID - an empty string is shown instead. Although it looks like a good idea (if no one sees the WLAN it cannot be attacked), it is not helpful at all.

MAC ADRESS FILTERING: Like SSID hiding, MAC address filtering is also commonly used "security" mechanism.

Although it is better to use even weak protection than none at all, MAC address filtering can be easily broken by using MAC address spoofing technique.

WEP (Wired Equivalent Privacy)

Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks.

WEP Encryption

For each packet, a 24-bit initialization vector (IV) is chosen. The IV concatenated with the root key yields the per packet key. The CRC-32 is calculated over the data to be encrypted. The per packet key is then used to encrypt the data followed by the ICV using RC4 stream cipher. The (unencrypted) IV is transmitted in the header of the packet.

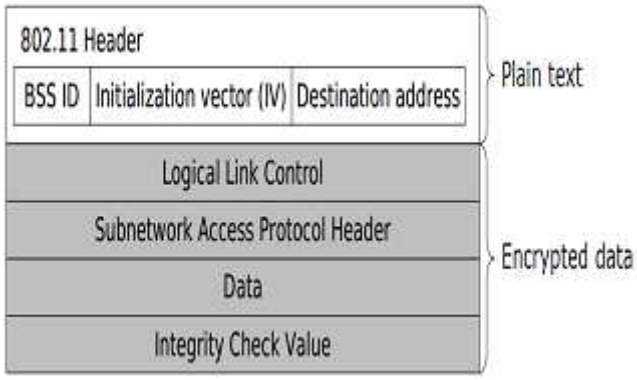

Figure 2: Simplified WEP Frame

WEP Decryption

The initialization vector (IV) is unencrypted in the header. The IV is appended to the root key. The combination of IV and the root key is used as an input for the pseudo-random number generator to generate a bit sequence. This sequence is XORed with the encrypted data plus ICV to decrypt the data. The ICV calculation then is run. If the value matches the value of ICV in the incoming frame, the data is considered to be valid.

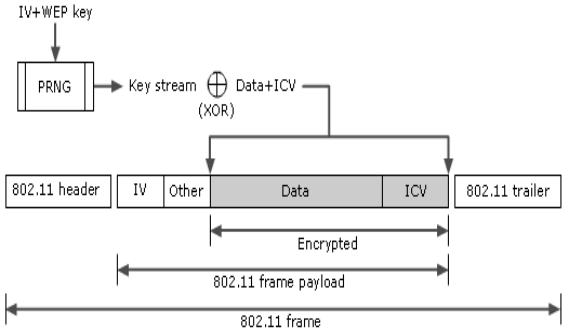

Figure 3: WEP Encryption

WPA (WIFI PROTECTEC ACCESS)

The basic principle of WPA could be simplified as follows: transfer the data decrypted by Temporary Key Integrity Protocol before somebody can decrypt the key. While WEP was using single pre-shared key for all encryption, WPA changes the unicast encryption key for every frame and each change is synchronized between the wireless client and the wireless AP. For the global encryption key, WPA includes a facility for the wireless AP to advertise changes to the connected wireless clients.

WPA features two different operation modes:

- WPA-PSK (Pre-Shared Key) mode
- WPA Enterprise mode

WPA Encryption

WPA needs following values in order to encrypt a wireless data frame:

- Initialization vector (IV)
- Data encryption key
- Source and destination addresses (SA, DA)
- Priority field value
- Data integrity key

WPA Decryption

The WPA decryption process can be described as follows: The IV is extracted from the IV and extended IV fields. The IV, DA and the Data encryption key are used as the input for the key mixing function to produce the per-packet key. IV and per packet key are used as the input for RC4 PRNG function to generate key stream of the same size as the encrypted data, MIC and ICV. The key stream is XORed with the encrypted data, MIC and ICV to produce unencrypted ICV, MIC and the data. The ICV is calculated and compared with the value of unencrypted ICV.

WPA2

In September 2004, the Wi-Fi Alliance introduced Wi-Fi Protected Access 2 (WPA2),which is the second generation of WPA security. WPA2 still uses PSK authentication but instead of TKIP encryption it uses enhanced data encryption: a specific mode of

The Advanced Encryption Standard (AES) known as the Counter Mode Cipher Block.

WPA2, similarly to WPA, offers two modes of operation:

- WPA2-PSK (Pre-Shared Key) mode
- WPA2 Enterprise mode

WPA2 Encryption

- Encrypt a starting 128-bit block with data integrity key and AES.
- In the next step, XOR Result1 with next 128-bit block to produce XResult1.
- Encrypt XResult1 with AES and data integrity key
- XOR Result2 and the next 128-bit block of data.

WPA2 Decryption

Decryption process can be summarized in these 4 steps:

- Find the value of the starting counter from values in 802.11 header and MAC header.
- The starting counter value and the encrypted portion of the 802.11 payload are used as an input for the AES counter mode decryption algorithm with the data encryption key. The result is the decrypted data and MIC. To produce the decrypted data block, AES counter mode XORs the encrypted counter value with the encrypted data block.

- The starting block, 802.11 MAC header, CCMP header, data length, and padding fields are used as an input for the AES CBC-MAC algorithm with the data integrity key to calculate a MIC.
- To find out if the data is valid, compare the unencrypted MIC with the calculated value of MIC. If the values do not match, WPA2 discards data.

BRUTE FORCE METHODOLOGY

The following chart illustrates how the optimized brute-force attack works:

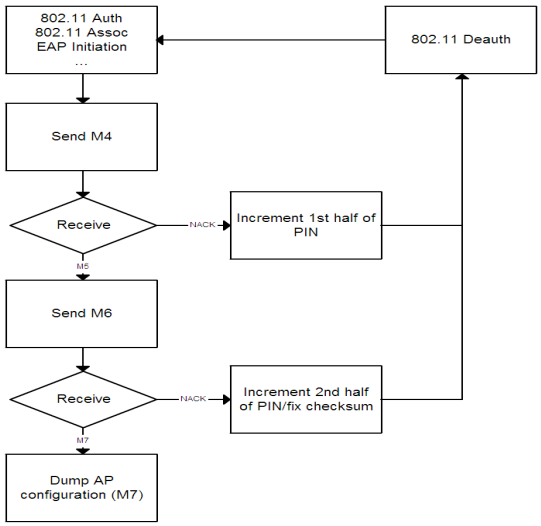

Figure 4: Brute Force Attack Chart

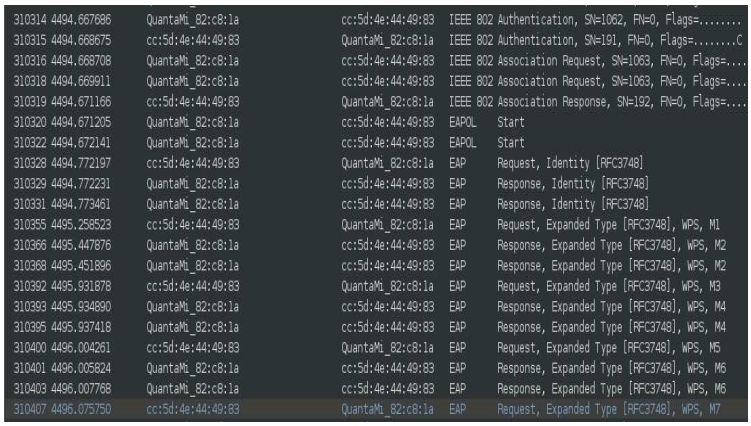

Figure 5: Example of Brute Force Attack

CONCLUSIONS

In the research work it is observed that many organizations are currently deploying wireless networks typically to use IEEE 802.11b protocols, but technology used is not secure and still highly susceptible to active attacks and passive intrusions. Currently available security protocols like WEP, WPA and WPA2 have some advantages and disadvantages and also there are some vulnerability exists in these security protocols. Various types of security attacks are possible as explained in the previous sections

Wifi Security provided a preview of mechanisms used for securing wireless networks.. This provided us useful information which we used in the next chapter, which was dedicated to WLANs encryption standards and mechanisms. In the chapter we discussed how does each of the standards work: improvements compared to previous standard, encryption process, decryption process, flaws and possible attacks.

ACKNOWLEDGEMENTS

We would like to acknowledge and extend my heartfelt gratitude to the Mr. Rudra Pratap Ojjha and Mr. Santosh Upadhyay for hosting this research, making available the data and valuable comments.

REFERENCES

1. M. Gast, 802.11 Wireless networks: The definitive guide. O'Reilly & Associates, Inc., Sebastopol, 2002.
2. What is 802.11 wireless?." http://technet.microsoft.com/en-us/library/ cc785885(v=ws.10).aspx.
3. T.Nghi, \Wireless local area network."http://www.netlab.tkk.fi/opetus/s38118/s00/tyot/25/index.shtml.
4. A. M. A. Naamany, A. A. Shidhani, and H.Bourdoucen, \IEEE 802.11 wireless lan security overview," in IJCSNS International Journal of Computer 138 Science and Network Security, pp. 138{155, 2006.
5. Q. Docter, E. Dulaney, and T. Skandier, CompTIA A+ Complete Study Guide: Exams 220-701 (Essentials) and 220-702 (Practical Application). Sybex, 2009.
6. DHCP starvation attack." http://www.networkdictionary.com/ networking/DHCPStarvationAttack.php.
7. Cisco unified wireless network architecture| base security features." http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch4_Secu.html.
8. S. DeFino, B. Kaufman, N. Valenteen, and L. Greenblatt, Offcial Certified Eth-ical Hacker Review Guide. Cengage Learning, 2009.
9. M. Stxhlberg, \Radio jamming attacks against two popular mobile networks," 2000.
10. A. Mousa and A. Hamad, \Evaluation of the RC4 algorithm for data encryption,"Proc. Of International Journal Computer Science & Applications, vol. 3, no. 2,2006.
11. B. Bing, The world wide Wi-Fi : technological trends and business strategies.John Wiley & Sons, Inc, 2003.
12. H. Berghel and J. Uecker, \WiFi attack vectors," Communications of the ACM, vol. 48, no. 8, pp. 21{28, 2005.
13. K. Hulin, C. Locke, P. Mealey, and A. Pham, \Analysis of wireless security Vulnerabilities, attacks, and methods of protection," Information Security Semester Project, 2010.
14. E. Tews and M. Beck, \Practical attacks against WEP and WPA," in Proceedings of the second ACM conference on Wireless network security, pp. 79{86, ACM, 2009.
15. E. Tews, \Attacks on the WEP protocol," IACR Eprint Server, eprint. iacr. org,no. 2007/471, 2007.
16. B.Haines, Seven Deadliest Wireless Technologies Attacks. Syngress/Elsevier, 2010.

17. J. Wang, Computer network security : theory and practice. Springer, 2009.

18. J. Davies, \Wi-fiprotected access data encryption and integrity." http://technet.microsoft.com/en-us/library/bb878126.aspx.

19. J. Edney and W. A. Arbaugh, Real 802.11 Security: Wi-Fi Protected Access and 802.11i. Addison Wesley, 2004.

20. A. A. Vladimirov, K. V. Gavrilenko, and A. A. Mikhailovsky, Real 802.11 Security Wi-Fi Protected Access and 802.11i. Addison Wesley, 2004.

21. M. D. Ciampa, Security+ Guide to Network Security Fundamentals. Course Technology, Cengage Learning, 2012.