National Research Journal of Business Economics
Volume-5, Issue-1, Year-2018 **ISSN: 2349-2015**

A STUDY OF WIRELESS NETWORK SECURITY TECHNIQUES

Charanjeet Singh, Ramandeep Kaur

Gujranwala Guru Nanak Institute Of Management & Technology, Ludhiana, Punjab, India

Introduction

WLAN or Wireless Local Area Network is a term used for the networks in which a user can have a high bit rate network connection through a wireless (radio) connection. The WLAN networks are usually high in bit rate but relatively short in range. There are several standards that specify the different kinds of WLANs.The physical architecture of wireless networks uses Access Points (AP) to connect to the normal wired network and they provide wireless access to clients (e.g. laptops, PDAs) with WLAN Network Interface Cards (NIC). WLANs may also be set up between two devices with a NIC, and it is possible to use the WLAN technology to build larger ad hoc networks as well. The subsequent sections will review the various techniques that are usually employed to strengthen the security in WLANs along with their potential merits and vulnerabilities.

1. Wired Equivalent Privacy (WEP)

Eavesdropping on a wireless network is much easier than on a wired network, so 802.11a and b standards introduced an encryption algorithm called Wired Equivalent Privacy (WEP) Wired Equivalent privacy was intended to give wireless users security equivalent to being on a wired network. It is the encryption scheme which combines packet's data payload with encryption key.

WEP uses a pre-established shared secret key called the base key, the RC4 encryption algorithm and the CRC-32 (Cyclic Redundancy Code) checksum algorithm as its basic building blocks[1]. In WEP there are two levels of encryption which are de needed by the key length. The key package can be either 64 or 128 bits long, of which 24 bits always contain the unencrypted initialization vector. Thus WEP encryption is either 40 or 104 bits strong (although some-times referred to as 64 or 128 bit encryption).

The RC4 algorithm was designed by Ron Rivest in 1987. It's a symmetric stream cipher algorithm that was publicized in 1994 when someone posted it into several cryptology newsgroups. The algorithm consists of two parts, the Key Scheduling Algorithm (KSA) and Pseudo Random Generation Algorithm (PRGA), whose weaknesses are discussed in more detail by Fluhrer and Shamir. [2] Although WEP is easy to implement. WEP can provide basic security for WLAN applications. In WEP transmission privacy is ensured through RC4 encryption as shared secret key has to be used for decryption. Transmission integrity is ensured by the CRC-32 checksum.WEP has been widely criticized for a number of weaknesses that include Key management and key size. The IV is too small[3,4].

2.Access Control with SSIDs

SSID(Service Set Identifier) is used to differentiate networks from one another. SSID settings are considered first level of security on the network[5].Following some security parameters regarding SSID help in ensuring better wireless security that include: changing the default SSID,not setting SSID to some meaningful information and by disabling "Broadcast SSID"option[6,7].

3.MAC address Filtering

MAC address of network card is the 12 digit hex number that is unique to each & every NIC in this world. By limiting the access to AP to only those MAC addresses of authorized devices, we can easily shut out everyone who should not be on our network. In wireless network each AP maintains a table of MAC addresses of different clients. Only those clients are allowed to access the network whose MAC address is in the list[8].

4. 802.1x Security

802. 1x is defined by IEEE as a port- based access control method that provides a better way to control access to network ports[9]. 802.11 AP responds by enabling the port for passing only EAP packets from client to authentication server. This AP blocks all other traffic like DHCP, HTTP, POP3 packets until AP can verify the client's identity using an authentication server.

There are several implementations of EAP, including:

1. Transport Layer Security (EAP-TLS): developed by Microsoft and used in 802.1X clients for Windows XP, EAP-TLS provides strong security, but requires each WLAN user to run a client certificate.
2. Lightweight EAP (LEAP): developed by CISCO and used in their Aironet solution, LEAP supports dynamic WEP key generation and provides for fixed password user authentication.
3. Protected EAP (PEAP): co-developed by CISCO, Microsoft and RSA Security, PEAP does not require certificates for authentication. It supports dynamic WEP key generation and provides options for password, token or digital certificate-based user authentication.
4. Tunneled Transport Layer Security (EAP-TTLS): developed by Funk Software and Certicom as a competing standard for PEAP, EEAP-TTLS supports password, token or certificate-side user authentication. Unlike EAP-TLS, EAP-TTLS requires only the server to be certified.

5. 802.11i -CCMP

IEEE 802.11i defines Robust Security Network (RSN)" [10] that is aimed solving the problems in 802.11b and WEP which include Poor Privacy, lack of encryption key management, Weak authentication and authorization and no Accounting. CCMP stands for the Counter-Mode-CBC-MAC Protocol. Like TKIP, the long-term solution addresses all known WEP deficiencies.CCMP uses AES for encryption instead of RC4.CCMP merges two well-known and widely deployed techniques. CCMP uses counter mode for encryption i.e. for privacy and the Cipher Block Chaining Message Authentication Code (CBC-MAC) for

integrity and protection. Figure 1 presents the comparison between WEP,TKIP and CCMP.
Figure1: Comparison between WEP, TKIP and CCMP.

	WEP	TKIP	CCMP
Cipher Key Size(s)	RC4 40- or 104-bit Encryption	RC4 128-bit encryption, 64-bit authentication	AES 128-bit
Key Lifetime Per-packet key	24-bit wrapping IV Concatenate IV to base key	48-bit IV TKIP mixing function	48-bit IV Not needed
Integrity Packet Header	None	Source and destination addresses protected by Michael	CCM
Packet Data Replay detection	CRC-32 None	Michael Enforce IV sequencing	CCM Enforce IV sequencing
Key Management	None	IEEE 802.1X	IEEE 802.1X

6. WPA

Wi-Fi Protected Access is a WLAN data encryption method that uses TKIP to alleviate WEP key flaw by generating a new 128-bit per packet transmitted. WPA enhances WEP by adding a rekeying mechanism to provide a fresh encryption and integrity key. Temporal keys are changed for every 10,000 packets. This makes it much harder to crack TKIP keys than with WEP. In WPA, a temporal encryption key, transmit address and TKIP Sequence Counter (TSC) form the input to the RC4 algorithm that generates a key stream. MAC Service Data Unit (MSDU) and Message Integrity Check are combined using the Michael algorithm. The combination of the MSDU and the MIC is fragmented to generate MAC Protocol Data Units, which is MPDU. From the MPDU, a 32-bit Integrity Check Value is calculated for the MPDU. The combination PDU and the ICV is bit-wise exclusive ORed with a key stream to produce the encrypted data. The IV is added to the encrypted data to generate the MAC frame.WPA] is not a very strong algorithm and has certain vulnerabilities[12]: The WPA uses a RC4 cryptography algorithm instead of an Advanced Encryption Standard (AES) that is more secured and encrypt better. Brute force attack can also be carried out on the WPA. The WPA is also open to Do S attacks. The setup or configuration process is complicated. In the WPA, several attacks are common to it such as the Beck-Tews Attack, Ohigashi-Morii Attack, Micheal Reset Attack, and WPA-PSK Attack.

7.WPA2

This is an enhancement to WPA. It uses AES algorithm for encryption which is stronger than TKIP. AES in combination with Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) provide high level security to WLAN. The CCMP algorithm creates message integrity code (MIC) to protect data integrity. WPA2 supports both Enterprise mode and Personal mode. WPA2 Personal uses a set of password. WPA2 Enterprise uses EAP and a RADIUS server for centralized client authentication using multiple authentication methods such as token cards, Kerberos, and certificates.[13-15].

Conclusion

The use of wireless local area networks is growing rapidly. As wireless local area networks become integral parts of enterprise-level networks, it becomes imperative that the wireless components of the network be as secure as the wired network. With careful planning and due diligence, a wireless network can be as secure as a wired network. Human factors are as important as technical factors in ensuring wireless security. Achieving secured WLAN requires implementing security at all layers which include wireless signal security, connection security, data protection, device security, network protection, and end user protection. Organizations should perform a risk analysis of their network, develop, and implement relevant and comprehensive security policies throughout their network. The result of the discussion shows that there is no one solution that is the best. However a user can ensure better security by using combination of all these security techniques.

REFERENCES

1. Ailus S. and Hedberg J. ***T-110.452 Practical security of IEEE 802.11b*** T-110.452Special seminar course for practical information systems security Telecommunications Software and Multimedia Laboratory Helsinki University of Technology, March 2003.
2. Fluhrer, Mantin and Shamir ***Weaknesses in the Key Scheduling Algorithm of RC4*** http://www.drizzle.com/ aboba/IEEE/rc4_ksaproc.pdf
3. Takahiro Fujita, Kiminao Kogiso, Kenji Sawada, & Seiichi Shin, "Security Enhancements of Networked Control Systems Using RSA Public-Key Cryptosystem", 978-1-4799-7862-5/15©2015 IEEE.
4. Airsnort http://airsnort.shmoo.com/ The Shmoo Group, 2003.
5. Rager, Anton ***Wepcrack - An 802.11 key breaker***
6. IEEE 802.11 work group***IEEE 802.11 Wireless Local Area Networks*** http://grouper.ieee.org/groups/802/11/ The Institute of Electrical and Electronics Engineers, Inc. (IEEE), 2003.
7. Banks, L. T., Defining Best Practices for Designing and Implementing 802.11 Wireless Security, Vigilar Inc., 2002.
8. United States Computer Emergency Readiness Team (US-CERT), Vulnerability Note VU#106678: IEEE 802.11 Wireless Network Protocol DSSS CCA Algorithm Vulnerable to Denial of Service, http://www.kb.cert.org/vuls/id/106678, 2004, Last accessed July 1, 2004.

9. A. R. Vaidya and S. Jaiswal, "Secure and Flexible Communication Technique: Implementation Using MAC Filter in WLAN and MANET for IP Spoofing Detection," International Journal of Computer Networks and Wireless Communications, vol. 3, no. 4, pp. 519-525, 2016.
10. RFC 2284, PPP Extensible Authentication Protocol (EAP), http://www.ietf.org/rfc/rfc2284.txt, 1998, Last accessed July 1, 2004.
11. Stubblefield, A., Ioannidis, J. and Rubin, D. (2001). Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. AT&T Laboroties and Rice. Available:http://www.uninett.no /wlan /download/wep_attack.pdf.
12. Mone, G. (2013). Future-Proof Encryption. Communications of the ACM, Vol. 56(11), pp. 12-14 DOI. 10.1145/2524713.2524718.
13. *Comparative Analysis of Wireless Security Protocols: WEP vs. WPA.* https://www.researchgate.net/publication/287197979_Comparative_Analysis_of_Wireless_Security_Protocols_WEP_vs_WPA
14. Sari, A. and Rahnama, B. (2013) Addressing Security Challenges in WiMAX Environment. Proceedings of the 6th International Conference on Security of Information and Networks, Aksaray, 26-28 November 2013, 454-456. http://dx.doi.org/10.1145/2523514.2523586
15. Miller, B. (2008) WPA2 Security: Choosing the Right WLAN Authentication Method for Homes and Enterprises. Global Knowledge.
16. Sari, A. and Rahnama, B. (2013) Simulation of 802.11 Physical Layer Attacks in MANET. 2013 5th International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN), Madrid, 5-7 June 2013, 334-337.