

Building a secured wireless LAN

Rajni Pamnani, Pramila Chawan
 Department of computer Technology,
 Veermata Jijabai technological Institute,
rajni_as@yahoo.com
pmchawan@vji.org.in

Abstract

The security of wireless LANs has been a source of concern for businesses and individuals who are aware of its advantages due to its flexibility. With the increase in the use of wireless LANs for enterprises and homes, where information assets are shared continually, security is of the essence. With the increase in ecommerce and e-services, there is the risk of identity and credit card theft. This Paper discusses the various security protocols used in wireless LANs and how effective they are in keeping wireless LANs secure. Our work focuses on using existing protocols, standards to implement a secure wireless LAN. It introduces two new enhancements that will soon improve upon WEP.

Key words: 802.11 Protocols, TKIP, WEP, Wi-Fi protected access

1. Introduction

Wireless LAN (WLAN) technology is more secure, robust, and affordable than ever before. That's why more enterprises are taking advantage of the mobility and productivity benefits that WLANs provide. However, WLAN success is not as simple as plugging in an access point (a wireless "hub") and handing out wireless cards. It requires careful consideration of your network and user requirements, preparation, and a sound deployment and security strategy. wireless is a shared medium, not a switched medium. The advantages of WLANs are widely touted. They offer users anytime, anywhere network access and help IT departments cut cabling costs and simplify labor-intensive installations. But in today's budget-tightening economy, the benefits of such technologies must be tested and proven before they are implemented.

Wireless "hot spots" based on 802.11b are also popping up in hotels, airports, convention centers, and coffee shops worldwide, making it an important, emerging market for service providers as well. Interoperability of 802.11b products from different vendors is ensured by an independent organization called the Wireless Ethernet Compatibility Alliance (WECA), which identifies compliant products under its "Wi-Fi" Brand. With Wi-Fi membership boasting more than 140 companies, spanning component

manufacturers, equipment vendors, and service providers, the future of the 802.11 standard is secured.

2. Traditional Security

Wireless security can be broken into two parts: Authentication and encryption. Authentication mechanisms can be used to identify a wireless client to an access point and vice-versa, while encryption mechanisms ensure that it is not possible to intercept and decode data. For many years, MAC access control lists have been used for authentication, and 802.11 WEP has been used for encryption. Much attention has been focused recently on the security aspects of existing Wi-Fi (IEEE 802.11) wireless LAN systems.

3. Security Protocols and Enhancements

3.1 Wired Equivalent Privacy (WEP)

In 1997, WEP was developed by the 802.11b task force with the introduction of wireless technology, and was the first encryption protocol to be deployed with wireless networks. WEP incorporates two types of protection, a secret key and encryption. WEP stands for Wired Equivalent Privacy and protects wireless communication from eavesdroppers. WEP also prevents unauthorized access to wireless networks. The WEP algorithm works on the basis of a secret key shared between a mobile device (e.g. PDA, cell phone, tablet PC) and an access point [5]. Packets are encrypted using the key before transmission. An integrity check ensures that packets are not changed during the transmission. Although WEP does not purport to state how the key is shared between sender and receiver, most systems share a single key among all mobile devices and wireless access points. More sophisticated key management techniques can be used to help defend from the attacks we describe.

WEP uses the RC4 encryption algorithm, known as a stream cipher, which expands a short key into an infinitely long random character stream.

3.1.1 Problems with WEP

WEP has several serious inherent problems. It does not meet its fundamental security goals of wired equivalent confidentiality. It also fails to meet the expected goals for integrity and authentication.

WEP has two generic limitations. First, the use of WEP is optional, and as a result, many real installations never even turn on encryption. Second, by default, WEP uses a single shared key common to all users of a WLAN, and this common key is often stored in software-accessible storage on each device. If any device is lost, stolen or compromised, the only solution is to change the secret key in all of the remaining devices. Since WEP does not include a key management control, distributing the new secret key to all the users is a tasking process.

In practice, the most serious problem with WEP is that its encryption keys can be recovered through cryptanalysis. It was discovered that a passive attack could recover the RC4 key after eavesdropping on the network for a few hours and collecting 100,000-1,000,000 packets. A hacker could use an XOR function to mathematically link two packets of a session that have been processed with the same IVs, i.e. identical RC4 keys, which can be used to recover the key.

3.2 802.11i and its Improved Version

The 802.11 Security Task Group that is creating the 802.11i standard is working to specify stronger encryption algorithms for use in 802.11 networks. In the current draft specification, a strengthened version of the RC-4 / per-frame encryption algorithm, and a 128-bit AES encryption algorithm are proposed. Due to the physical vulnerability of wireless links, DoS attacks always exist through frequency jamming, network jamming, or other exploits. However, we improve the 802.11i protocol to achieve DoS resistance in the Link Layer. In order to eliminate the DoS attacks by Association Request flooding, it is better to perform authentication before association. The authentication and key management suite negotiation should be verified as soon as possible. The management frames should be authenticated to improve security, and some control frames can also be authenticated if necessary. An appropriate failure recovery scheme is implemented to improve the efficiency of the overall protocol.

3.3 Wi-Fi Protected Access

As an intermediate solution that can be applied to existing WLAN hardware, the Wi-Fi Alliance has

adopted Wi-Fi Protected Access (WPA). WPA is a specification of standards-based, interoperable security enhancements that strongly increase the level of data protection and access control for existing and future wireless LAN systems. Designed to run on existing hardware as a software upgrade, Wi-Fi Protected Access is derived from, and will be forward compatible with the upcoming IEEE 802.11i standard. When properly installed, it will provide wireless LAN users with a high level of assurance that their data will remain protected and that only authorized network users can access the network. Wi-Fi Protected Access was created with several goals in mind:

1. A strong, interoperable security replacement for WEP
2. Software upgradeable to existing Wi-Fi certified client products.
3. Applicable for both home and large enterprise users
4. Available immediately.

To meet these goals, 802.11 authentication and encryption were improved using parts of the 802.11i standard draft.

3.3.1 Enhanced Data Encryption through TKIP

To improve data encryption, Wi-Fi Protected Access utilizes the Temporal Key Integrity Protocol (TKIP). TKIP provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. Through these enhancements, TKIP addresses all of WEP's known vulnerabilities

3.3.2 Enterprise-level User Authentication via 802.1x and EAP

WEP has almost no user authentication mechanism. Wi-Fi Protected Access user authentication is implemented using 802.1x and the Extensible Authentication Protocol (EAP). Together, these technologies provide a framework for strong user authentication. This framework utilizes a central authentication server, which employs mutual authentication so that the wireless user does not accidentally join a rogue network.

3.3.3 Wi-Fi Protected Access and IEEE 802.11i Comparison

Wi-Fi Protected Access will be forward compatible with the IEEE 802.11i security specification currently under development. Wi-Fi Protected Access is a subset of the current 802.11i draft and uses certain

pieces of the 802.11i draft that are ready to bring to market today, such as 802.1x and TKIP. The main pieces of the 802.11i draft that are not included in Wi-Fi Protected Access are secure IBSS (Ad-Hoc mode), secure fast handoff (for specialized 802.11 VoIP phones), secure de-authentication and disassociation, as well as enhanced encryption protocols such as AES-CCMP. These features are either not yet ready for market or will require hardware upgrades to implement.

4. 802.1x Secured Wireless Network Components

Understanding 802.1x requires knowing the names of the different components that make up an 802.1x-secured wireless network. Figure shows the location role of each one of these terms in the authentication process.

Supplicant: End User System seeking access to the network

Authenticator: Controls access to the network (access point)

Authentication Server (RADIUS Server): Authenticates the end user, negotiates key material with the end user, controls access to the network via the authenticator.

EAP(Extensible Authentication Protocol): A secure protocol for negotiating other security protocols.

EAPOL (EAP Over LAN) : The version of EAP that is used over wireless networks.

PAE (Port Access Entity) : PAEs are similar to toggle switches. When the switch is open, no traffic is allowed to pass except for 802.1x traffic. After authentication is successful, the switch closes and user data is allowed to pass.

4.1 802.1x Encryption Method

Attacks like the one launched by AirSnort are the most troublesome for 802.11 networks, however, they are also the easiest to prevent using two common mechanisms: ORiNOCO's weak key avoidance (WEPplus), together with the key rotation mechanism built into the 802.1x standard and ORiNOCO access points, make it possible to create a secure wireless network.

In the existing pre-802.1x 802.11 specification, neither key distribution nor key rotation mechanisms are specified. With the exception of MD5, all EAP types provide a mechanism for the establishment of a session key at the station and the RADIUS server. This session key provides a secure means to periodically transport new encryption keys to the station, so that the keys used to encrypt user data can continuously and securely change.

5. Conclusion

WLANs offer new services that traditional wired LANs cannot provide, but they also introduce new security concerns. As wireless local area networks become integral parts of enterprise-level networks, it has become imperative that the wireless components of the network be as secure as the wired network. Although the early versions of WLANs were not designed for security, standards and methods are emerging for securing 2G broadband, enterprise-capable WLANs.

The WLAN industry has responded by creating WPA and 802.11i to address the issues in the long term, though these security solutions are not available today. Most of today's security requirements can be met with 802.1x, which provides a solution that is effective and has not yet been broken. With 802.1X and 802.11i protocols, there are now good choices for encryption and authentication. These emerging security features must be implemented in order to assure the security of information on the wireless networks. As the increase of e-commerce and e-services to both home and business users gathers momentum, the risk to these users of suffering loss of control of information-- interception, insertion, deletion, corruption and related physical assets will become of increasing concern both to individuals and to society in general. There is the need to incorporate wireless security into the curricula of information security programs to maintain the relevancy of students' knowledge in today's world.

References

- [1] Waheed, F. Muhiuddin, S. Ilyas, S.M., "Multi-Level Security for Wireless LAN", SCONEST 2005. Student Conference, August 2005.
- [2] Jiang L. Garuba, "Encryption as an Effective Tool in Reducing Wireless LAN Vulnerabilities", Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference, April 2008
- [3] Virendra, M. Upadhyaya, S. Wang, "GSWLAN: a new architecture model for a generic and secure wireless LAN system", Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC, June 2004
- [4] N. Cam-Winget, R. Housley, D. Wagner and J. Walker, "Security flaws in 802.11 data link protocols", May 2003.
- [5] K.J. Hole, E. Dyrnes, and P. Thorsheim. Securing Wi-Fi networks. *Computer* Pages 28-34. July, 2005.
- [6] "Wireless Network Security", ORiNOCO security paper v2.2
- [7] Brewer, Borisov, et al, "802.11 Security", <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>