Wireless Security Techniques: An Overview

Bhagyavati
Columbus State University
4225 University Avenue
Columbus, GA 31907
+1 706-565-3519
bhagyavati@colstate.edu

Wayne C. Summers
Columbus State University
4225 University Avenue
Columbus, GA 31907
+1 706-568-2410
summers_wayne@colstate.edu

Anthony DeJoie
Telcordia Technologies, Inc.
1 Telcordia Drive
Piscataway, NJ 08854
+1 732-699-2959
tony@research.telcordia.com

ABSTRACT

This paper provides a survey of the different techniques that can be used to strengthen security in wireless local area networks (WLANs). The first generation of WLANs were deployed by small businesses and individuals at homes. The second generation of WLAN products are more secure than those of the first generation. Second generation broadband wireless networks are considered to be enterprise-level networks providing more capacity and coverage than first generation home- and small business-based WLANs. However, security remains the most critical area of concern in both first generation and second generation WLANs. In this paper, we provide a survey of second generation broadband WLANs technologies and focus on security techniques.

Categories and Subject Descriptors

K.6.5 Security and Protection [**Management of Computing and Information Systems**]: Security and Protection – Authentication, Invasive software (e.g., viruses, worms, Trojan horses), Unauthorized access (e.g., hacking, phreaking) (D.4.6, K.4.2)

General Terms

Security, Human Factors.

Keywords

Wireless security, information assurance, information security curriculum, curriculum development.

1. INTRODUCTION

Most wireless networks today use the IEEE 802.11 standard for communication. The IEEE 802.11b has become the de-facto standard for wireless networking technology among both small business and home users. The IEEE 802.11b specification allows for the theoretical transmission of approximately 11 Mbps of raw data at indoor distances from several dozen to several hundred feet, and outdoor distances of several to tens of miles as an unlicensed use of the 2.4 GHz wireless band. The network devices typically are equipped with the Wired Equivalent Privacy (WEP) data encryption, based on the 64-bit RC4 encryption algorithm as defined in the IEEE 802.11b standard on wireless LANs. There are more expensive devices that are able to use 128-bit encryption. All the nodes must be at the same encryption level with the same key to operate.

There are several flaws in WEP making it unusable for high security applications. To further enhance wireless security, access points can sometimes be configured to only react to specific computers using the MAC address of the network adapter. 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 [4]. 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. Plain text is XOR'ed by the sender to generate cipher text, which is then transmitted. Although the cipher text can be obtained in transit, hackers usually cannot understand the content of the message because they do not have access to the key that was used by the sender for encryption. A trusted receiver, on the other hand, can decipher the contents of the message because it has a copy of the same key that was used by the sender to encrypt the message. However, if hackers modify the encrypted stream of data in transit, the receiver will receive incorrect data. If 2 such encrypted messages are intercepted by hackers, then XOR of the cipher text yields the XOR of the original messages. This knowledge can aid a determined and skillful hacker to mount statistical attacks to obtain the original plain text message. Due to these vulnerabilities, the encryption algorithm used by WEP is not the strongest to protect against all attacks.

Although WEP is limited in providing security, it does have defenses against both these attacks. To protect against modification of a packet during transmission, WEP uses an Integrity Check field. In order to discourage statistical attacks of the kind described above, WEP uses an Initialization Vector to augment the shared key between sender and receiver, and

InfoSecCD Conference'04, September 17-18, 2004, Kennesaw, GA, USA. Copyright 2004 ACM 1-58113-000-0/00/0004…$5.00.

produces a different RC4 key for each packet [4]. Since both these measures are implemented incorrectly in WEP, we still maintain that WEP alone is a poor choice in ensuring the security of wireless networks. This is one of the reasons why large businesses have been hesitatant to deploy wireless networks. In addition, corporations require broadband wireless; home WLAN products do not offer the coverage or capacity that enterprises need. The emergence of second generation broadband wireless products is changing this corporate mindset.

Second generation WLANs differ from the first generation in the following respects:

1. Relationship between coverage and capacity: While 1G WLANs emphasized coverage, 2G WLANs advocate capacity to support critical enterprise applications. The corporate philosophy is that coverage will follow by provisioning the correct number of access points (APs) if enough capacity can be designed in advance.
2. Focus on security: In 1G WLANs, security was a known weakness. In later 1G products, 128-bit static WEP made efforts at improving security. However, these WEP keys were easily hacked. Security remains one of the top factors why enterprises are reluctant to deploy WLANs; according to [6], end user installation of unmanaged access points has an 80% probability of causing exposure of sensitive information in more than 50% of enterprises. 2G WLANs tend to have an identity-based security management scheme.
3. Shift toward integrated network management: For security and mobility to co-exist in large enterprises, 2G WLANs need to seamlessly integrate the wired and wireless networks existing in the enterprise. In planning and architecting a WLAN for enterprise use, it is appropriate to centralize intelligence, especially security management, in the core, and distribute processing to the ends of the wired-wireless integrated network.

In order to deploy 2G WLANs effectively, corporate network administrators need proper planning tools in order to successfully design and implement a scalable, secure and integrated enterprise-wide network. In this paper, we focus on the security tools and techniques that network managers can use to deploy secure and integrated system

2. FIRST GENERATION WLANS

2.1 Security Issues

In order to strengthen the security of wireless devices, it is necessary to understand the security concerns experienced with 1G WLAN products. The three main security holes are:

1. equipment has security settings disabled by default,
2. minimal security is easily broken, and
3. rogue access points are easy to deploy and difficult to detect [5].

If users are to be productive no matter where they are, then WLANs have to be integrated seamlessly with the wired network in the enterprise; such WLANs need to meet the twin requirements of security and mobility.

Other issues also affect security in first generation WLANs. Human factors such as lack of awareness and lack of adherence to usage policies can cause loopholes in systems that have been secured in technical aspects. On the other hand, technical factors such as lack of encryption can cause loopholes in systems wherein the personnel are security-conscious and adhere strictly to security and usage policies.

2.2 Security Features

The minimal set of security features included in the 802.11b standard include:

1. Service Set Identifier (SSID): each access point has an SSID which identifies it to devices on the WLAN. The network can be configured so that clients are required to know the SSID of the access point before connecting to it.
2. Medium Access Control (MAC) address filters: the access point can be configured to accept connections only from clients with MAC addresses registered with the access point.
3. WEP encryption: The 802.11 standard included WEP as a mechanism for providing “confidentiality that is subjectively equivalent to the confidentiality of a wired LAN medium that does not employ cryptographic techniques to enhance privacy” [8].

2.3 Security Vulnerabilities

Several security vulnerabilities exist in 1G WLANs. Some of them include the following:

1. By default, the access point broadcasts its SSID in clear text. Even if the SSID broadcast is hidden, the client broadcasts the SSID to the access point while attempting to connect to it.
2. The MAC address of a valid client can be “sniffed” off the network and then spoofed by the rogue client.
3. As discussed in detail earlier, WEP encryption is easily cracked. WEP only authenticates the client. This allows a rogue access point to capture data sent by an authenticated client.
4. A rogue access point (AP) can be installed that will intercept traffic from wireless clients.
5. Man-in-the-middle attacks can be launched by forcing an access point off its channel and then spoofing the SSID of the access point.
6. WLANs are easily crashed by denial of service (DoS) attacks with methods ranging from flooding the access point with spoofed MAC addresses to using devices like 2.4 GHz cordless phones to cause excessive radio interference.
7. Recently, the US-CERT organization released an advisory about a vulnerability regarding unauthenticated 802.11 devices [15]. This vulnerability can be exploited by a remote hacker to cause denial of service.

2.4 Security Controls

Specific security methods that can be implemented to secure 802.11 wireless networks include any or all of the following [3]:

1. Turning off the broadcast SSIDs.
2. Introducing automated MAC-based access control mechanisms.
3. Enabling WEP encryption.
4. Lowering the power levels of the access points to limit the ability of hackers to connect from outside the specified boundary. This can also be accomplished by limiting connections to transmission rates of 11 Mbps and 5.5 Mbps.

3. SECOND GENERATION WLANS

Most breaches in security of wireless devices are a result of a variety of layer two vulnerabilities. Protection against these vulnerabilities require defense in depth, i.e. multiple controls. The IEEE 802.1X task group addresses the problems of network security and access control. The IEEE 802.11i group has mandated the use of the 802.1X suite of protocols to improve and standardize wireless encryption [7]. Such protocols include the Extensible Authentication Protocol (EAP), Protected EAP (PEAP) and Tunneled Transport Layer Security (TTLS), which supersede the weak WEP keys available for 1G WLANs. The 802.11i standard provides for using Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) to encrypt data on the wireless network.

3.1 Encryption and Virtual Private Networks

Although WEP is flawed, it is still valuable as a first line of defense. WEP can prevent most novice hacker attacks and possibly delay intrusions by unauthorized users. The Wi-Fi Alliance announced in October 2002 the industry-supported implementation of Wi-Fi Protected Access (WPA) as an interim protocol before AES becomes the standard [6]. However, with WPA, enterprise managers discovered that the WLAN was secure but not truly mobile and reflective of user demands. Due to user roaming and the resulting changes in static IP addresses, WPA required re-authentication, which posed problems with current 2G WLAN implementations. In addition, poorly chosen, short, human-readable passphrases used in WPA can be cracked with a robust dictionary attack offline and without access to the network [9]. However, identity-based schemes are being adopted, which provide security without sacrificing mobility.

The draft release of the IEEE 802.11i standard includes features to address several of the vulnerabilities inherent to WEP. TKIP is one of several such protocols being offered by various vendors. Although TKIP still uses the RC4 encryption algorithm, it removes the weak key problem by forcing a new key to be generated every 10,000 packets or 10 kb. It also hashes the initialization vector values that WEP sends as plaintext. TKIP includes a method for verifying the integrity of the data called the Message Integrity Check, which mitigates the vulnerability that allows a hacker to inject data into a packet in order to deduce the encryption key. AES is the newest encryption standard and is under review for inclusion in 802.11i. AES is the strong encryption replacement for Data Encryption Standard. According to the 802.11i standard, AES will replace WEP and RC4 encryption. This will require a hardware optimization to be able to handle the more robust algorithm.

Wireless networks are vulnerable by default. An additional safeguard that can be used to secure a wireless network is a Virutal Private Network (VPN). A VPN solution uses a combination of tunneling, encryption, authentication and access control. A VPN establishes a secure, encrypted network tunneled within a potentially hostile network like a wireless network.

3.2 802.1x Family of Protocols

802.1x is defined by IEEE as a port-based access control method that provides a better way to control access to network ports [1]. 802.1x does not specify an authentication method, although the most common approach for WLANs is EAP, which is a framework for a variety of authentication methods [11]. The specific method is determined by the client and access point during the authentication process. The EAP client (supplicant) contacts the access point (authenticator), which challenges the client for authentication information. The authenticator receives this information from the client and then passes it onto an authentication server for validation. No other communications from the client is permitted until the authentication server has validated the logon request. If the logon is accepted, the authentication server generates a WEP key specifically for the client and sends it through the access point to the client. The client is now permitted to access the network behind the access point.

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.

3.3 Wireless Gateways

Access points and WLAN clients are not designed to handle the large amount of overhead imposed by these additional layers of security. This becomes especially apparent as WEP's RC4 encryption is replaced by the more robust AES encryption. One solution that is being implemented is the wireless gateway.

Instead of access points connecting directly to the internal network, they are collectively connected to a device that contains the additional security levels where encryption and authentication are implemented. This configuration has the added advantages of simplifying roaming between access points without requiring additional authentication and the ability to implement Quality of Service at a single point.

3.4 Policies, Training and Awareness

No matter how much technology is employed at securing a wireless network, it will not be effective unless there are adequate policies in place along with security awareness training. Just as an enterprise has a security policy for a wired network, it should also have a strong policy on securing its wireless network. Important components of such a policy would include the following:

1. Physical location of access points: Suggestions range from concealing the access points to avoid vandalism, to shaping the radio waves by appropriate positioning of the antenna, to adjusting the power levels to prevent the signal from "bleeding" outside.
2. Logical location of access points: Access points should typically be placed in the DMZ screened from the corporate network by a properly configured firewall.
3. Rogue access points: A ban should be enforced on rogue access points. Consequences for violators should be stringent and strictly enforced.
4. Peer-to-peer mode: The ad-hoc or peer-to-peer mode on clients should be disabled by default.
5. Configuration: Properly configuring all devices, i.e. encryption, authentication and SSID is essential.
6. Interoperability: Requiring that standard equipment be purchased from a single vendor wherever possible will increase interoperability and compatibility.
7. Site surveys: Frequent site surveys to locate any rogue access points and clients set up in ad-hoc mode.
8. Monitoring: Frequent monitoring of the logs to ensure that intrusions have not occurred.
9. Updates and patches: Patch management policies are important to obtain timely updates.
10. Other: References to other security policies to ensure consistency and integration with wired networks.

4. DISCUSSION

4.1 Factors Affecting Deployment

Current factors affecting the deployment of wireless networks in organizations include security issues, lack of coverage, lack of capacity and control and usage issues. Factors affecting the deployment of 2G wireless include capacity and control issues. For example, many organizations deploy wireless technologies to supplement the existing wired infrastructure due to perceived lack of coverage issues. However, technologies such as those specified by the IEEE 802.11a and 802.11g high-speed standards have mitigated somewhat the lack of coverage and bandwidth issues. But lack of capacity still remains a concern. The other concern is security and usage issues. For instance, control over airwaves, dissemination of awareness training and propagation of security and appropriate use policies and guidelines are major concerns in organizations seeking to roll out wireless technologies.

4.2 Issues Affecting Curriculum Development

An obvious question is the fit of these factors into the information security curriculum as taught in schools and universities. Questions such as the following naturally arise out of a discussion of wireless technologies and factors involving their successful deployment. How can students be trained to be current when they enter the marketplace? How can Computer Science curricula adjust to reflect wireless awareness in the variety of career areas? Where do the issues discussed in this paper fit into the curriculum? What assignments and hands-on exercises will the student benefit from to better understand the material and apply it in their future jobs?

First, students in all areas of Computer Science need to become aware of security issues, not just surrounding wireless technologies, but also those embedded in wired networks, the existing infrastructure and system programming. Although some students may intend to specialize in non-security related areas, information security and assurance affects all aspects of computing. Second, instructors need to be trained in the latest information assurance technologies by attending training camps and keeping abreast of the latest developments in the field. A strong commitment is required from the administration to keep the knowledge of the educators current in order to enable top-down dissemination of relevant awareness.

Third, computer and network security topics can be incorporated into many traditional Computer Science courses at the undergraduate level, such as Operating Systems, Database Management Systems, Programming Principles, Software Engineering and Network Computing. Fourth, there needs to be at least a couple of courses focusing solely on network and infrastructure security, and information assurance. Wireless security can be incorporated into both these courses at the undergraduate level, and perhaps an advanced course devoted exclusively to wireless networking and security issues can be part of the graduate curriculum. We feel that this topic is current and timely, and highly relevant to the teaching and practice of information security curricula.

The main challenge in curriculum development of wireless security courses is the creation of relevant hands-on assignments. Because information security and wireless networking skills are perceived by students to be important for their future careers in business and industry, they want examples of "real" assignments, not trivial or academic ones. In our courses, we tend to develop both theoretical and hands-on assignments. While theoretical assignments can take the form of creating security plans and analyzing different plans in organizations, hands-on exercises extend this learning experience.

An example of a hands-on assignment involving wireless security asks students to compare security plans of different organizations in terms of their technical effectiveness. Another example is to ask students to enumerate the components needed to set up a simple wireless network. After this assignment is submitted, the common components are distributed and students are then asked to configure a wireless network based on their previous research. Yet another example of a real-life assignment could involve 2 teams of students – one team to secure a wireless network, and the other to try to attack and penetrate the first team's defenses.

New courses will need to be created continually to meet new developments in security and information assurance. Some new courses that have been developed at our university include information assurance, computer forensics and risk assessment. Several new and emerging topics are interdisciplinary in nature; for example, computer forensics requires knowledge of computers and legal issues, and risk assessment requires a mix of business and technical skills. Educating instructors in multiple disciplines who will then disseminate the knowledge to students is the key to ensuring currency in the information security curriculum.

4.3 WLAN Vs. LAN Security

A wireless LAN can be as secure as a wired LAN if security guidelines are implemented and enforced strictly. Various categories of factors affect information security, regardless of whether the information is transmitted through wired or wireless channels. For instance, human factors such as user awareness and operator carelessness are as important as technical factors such as encryption and firewalling wireless gateways. Before implementation of security policies, the organization must plan for various contingencies and vulnerabilities. After a plan has been designed, administrators and users should be trained in the procedures and made aware of the penalties for violations of the policy. Then the plan can be implemented throughout the organization. If the existing wired infrastructure is reasonably secure, then the wireless security procedures need to be integrated with the existing security guidelines for the wired network. In order to maintain currency of information security curricula, wireless security topics need to be included in a separate course or as major components in an existing course.

5. CONCLUSIONS

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. Although the early versions of WLANs were not designed for security, standards and methods are emerging for securing 2G broadband, enterprise-capable WLANs. 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. 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. As educators in information security programs, we need to incorporate wireless security into our curricula to maintain the relevancy of our students' knowledge in today's world.

6. REFERENCES

[1] 802.1x - Port Based Network Access Control, http://www.ieee802.org/1/pages/802.1x.html, 1998, Last accessed July 1, 2004.

[2] Aventail, Practical solutions for securing your wireless network, Aventail Technical White Paper, http://www.bitpipe.com/data/detail?id=1070473161_825&type=RES&x=1250903286, 2003, Last accessed July 1, 2004.

[3] Banks, L. T., Defining Best Practices for Designing and Implementing 802.11 Wireless Security, Vigilar Inc., 2002.

[4] Borisov, N., Goldberg, I. and Wagner, D. (In)Security of the WEP algorithm, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html, 2001, Last accessed July 1, 2004.

[5] Dulaney, K. and Margevicius, M., Wireless LANs for Notebooks Begin to Make Sense, Gartner's End-User Computing Research Note TG-17-3810, 2002.

[6] Everts, T., Editor, The Wireless LAN Book for Enterprises, Trapeze Networks, 2003.

[7] Geier, J., 802.1X Offers Authentication and Key Management, http://www.wi-fiplanet.com/tutorials/article.php/1041171, Last accessed July 1, 2004.

[8] Interlink Networks, Wireless LAN Security using Interlink Networks Secure.XS Software and Cisco LEAP Application Notes from Interlink Networks Resource Library, http://www.interlinknetworks.com/images/resource/Wireless_LAN_Security.pdf, 2002, Last accessed July 1, 2004.

[9] Moskowitz, R., Weakness in Passphrase Choice in WPA Interface, reprinted in Wi-Fi Networking News, http://wifinetnews.com/archives/002452.html, November 4, 2003, Last accessed July 1, 2004.

[10] Peikari, C. and Fogie, S., Wireless Maximum Security, SAMS, 2003.

[11] RFC 2284, PPP Extensible Authentication Protocol (EAP), http://www.ietf.org/rfc/rfc2284.txt, 1998, Last accessed July 1, 2004.

[12] Riley, S., Ask Us About… Security, http://www.microsoft.com/technet/archive/community/columns/security/askus/auas0303.mspx, February 2003, Last accessed July 1, 2004.

[13] RSA Security, Making Sense of WLAN Security, RSA Technical Whitepaper, http://www.rsasecurity.com/products/securid/whitepapers/MSWLAN_WP_0803.pdf, 2003, Last accessed July 1, 2004.

[14] Summers, W., Securing a Wireless Network, http://csc.colstate.edu/summers/Research/NetworkSecurity/wireless/wireless.html, August 2002, Last accessed July 1, 2004.

[15] 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.

[16] Vollbrecht, J. and Moskowitz, R., Wireless LAN Access Control and Authentication: http://www.interlinknetworks.com/images/resource/WLAN_Access_Control.pdf, a white paper from Interlink Networks Resource Library, http://www.interlinknetworks.com/images/resource/WLAN_Access_Control.pdf, 2001, Last accessed July 1, 2004.