Securing a Wireless Network

Jon Allen
Coordinator of IT Security,
Baylor University
PO Box 97268
Waco, TX 76798
(254) 719-4793
Jon_Allen@baylor.edu

Jeff Wilson
Senior Analyst/Programmer,
Baylor University
P.O. Box 97148
Waco, TX 76798
(254) 710 4615
Jeff_Wilson@baylor.edu

ABSTRACT
Driven by pressure to facilitate mobile computing, universities are plunging into wireless networking. Although wireless offers convenience and low-cost deployment, it lacks any inherent means of strong security. Common methods of securing wireless networks include WEP, VPN, MAC registration, IEEE 802.1x, and Firewalls. Each method offers some security, but at varying levels of complexity, convenience, cost effectiveness and completeness. Each security method has its own drawbacks.

Categories and Subject Descriptors
C.2.1[**WirelessCommunication**]
K.6.5[**Security and Protection**]

General Terms: Management, Measurement, Documentation, Performance, Design, Economics, Reliability, Experimentation, Security, Standardization, Languages, Theory, Verification.

Keywords WEP, VPN, 802.1x, 802.11i, EAP-MD5, EAP-TLS, EAP-LEAP, EAP-TTLS

1. INTRODUCTION
Driven by pressure to facilitate mobile computing, universities are plunging into wireless networking. Although wireless networks offer convenience and low-cost deployment, they lack any inherent means of strong security. Attempting to fill the security void, many companies have developed proprietary solutions for securing a wireless network. Other companies have chosen to modify their existing products to achieve wireless network security. Still others are depending on emerging technology standards to fill the wireless security void. While most of the solutions achieve some of the goals of wireless security, no solution has been able to achieve the security goals with a low cost and easy implementation.

2. REQUIREMENTS FOR WIRELESS SECURITY
Goals of wireless security have been adapted from the security schemes and methods of other information technologies. Due to the numerous security incidents over the past years, enterprises have begun to realize the importance of IT security. As a result, the IT industry has once again embraced some long known security concepts. A complete wireless security solution must be comprised of all three of the following key security elements: authentication, accountability, and encryption.

SIGUCCS'02, November 20-23, 2002, Providence, Rhode Island, USA.
ACM 1-58113-564-5/02/0011.

2.1 Authentication
Authentication encompasses the first piece of wireless security.. Many technologies are available to provide secure authentication schemes. Typically, universities have implemented robust authentication services to support their information technology infrastructures. Authentication can be comprised of one or more of the following categories:

a. something you know (i.e. username and password combinations)
b. something you are (i.e. biometric solutions such as fingerprint technology)
c. something you have (i.e. smart card and token technology)

The security of an authentication method is determined on a sliding scale. Low level authentication involves the use one of the authentication categories. The security strength of that authentication depends on the implementation of the method chosen. Something you have (option c) is probably the weakest method of single level security. A user losing the authentication device automatically makes their account vulnerable. As a result, a high level of administration may be required to maintain this category. Something you know (option a) is only as strong as the uniqueness of the information used and the confidentiality of that information. Users try to select passwords that are easy to remember. Those easy to remember passwords are also likely to be vulnerable to dictionary attacks. Something you are (option b) is a bit more secure but recently has been scrutinized in labs as easy to foil. Several research labs have determined that emulating biometric authentication technology may not be as difficult as originally believed. A large number of the high security authentication systems have now taken the approach of incorporating two of the categories for successful authentication. Something you have and something you know (a combination of options a and c) have led the pack in combination authentication systems.

2.2 Accountability
Accountability formulates the second piece of a strong wireless security system. University administrations, local and federal law enforcement all assume the ability of network administrators to track computer usage for accountability. Historically, the process of matching an IP address with a user was relatively easy. Wireless networks have added some challenges in this area. While an authentication scheme verifies that the user should be allowed on

the network, most do little in cases of tracking a user down. Few authentication services have native accounting systems that allow for easy backup of logs, tracking of users, and robust attribute fields. Radius is probably the most common accounting system used in conjunction with authentication services. Though originally designed for dialup services, it can be broadly adapted for many authentication services and environments. Baylor University chose to create a custom accounting service. As a result, we have been able to customize our logging for all the different student access networks on campus, including labs and wireless.

2.3 Encryption

The final key to a strong wireless security infrastructure is encryption. Lack of encryption constitutes the largest criticism against wireless networking. Wired equivalent privacy (WEP) has been widely cracked and criticized. IT professionals need to keep in mind that WEP was not designed with enterprise security encryption in mind. So that leads to the question, what technologies do provide strong encryption for a wireless network? First of all, the encryption method should be based on a public key infrastructure (PKI). PKI technology has quickly become the standard for the initiation and creation of secure encrypted sessions. Secondly, the method should use a high bit encryption scheme. The continuation of Moore's law results in 128bit encryption as the minimum for secure encryption tunnels. Finally, the algorithm used for the encryption must be well known and proven strong. A good example of this would be the 3-DES algorithm. The inclusion of all three of these components should contribute to a strong wireless encryption schema.

3. UNENCRYPTED SOLUTIONS

Current wireless solutions can be placed in one of two categories: unencrypted and encrypted. On the unencrypted side are technologies like MAC registration systems, firewalls and wireless gateways. Encrypted solutions include WEP, VPN and 802.1x/802.11i. In some cases, the unencrypted solutions can be combined with encrypted to form robust secure wireless networks.

3.1 MAC Registration

MAC Registration systems emerged out of a need to secure university residential networks. While many variations exist, the main theme is to restrict DHCP leases to a known set of MAC addresses. This known set may be obtained manually or through automated scripts running on a server. While these schemes are easy to implement and maintain, they lack in two of the three categories for wireless security. These systems weakly satisfy the authentication requirement. The systems verify that the network card has been registered by a valid user, but registration systems are unable to verify who the current user actually is. As a result, network administrators depend on stale registration logs to identify users. Accounting becomes impossible with registration systems. No session logons result in an inability to generate accounting logs, which in turn decreases the value of logging. Since these systems are designed for switched wired networks, encryption was not included; they provide acceptable security for dorm networks, but alone are unable to secure wireless networks.

3.2 Firewalls

The second pre-existing technology adapted to wireless networks is firewalls. Many enterprise firewall solutions include a method of network authentication, through HTTP, HTTPS, or telnet. The authentication request is forwarded to an authentication server (i.e. radius, active directory). Upon affirmative response, the firewall adds rules for the authenticated IP address. Rule timeout is tied to TCP activity or a timer. Authentication is session based and secure when executed over HTTPS. Though the attributes will be limited (username, timestamp and success/failure), the radius server will log the authentication attempt. Encryption is not included in the firewall solution; like other unencrypted schemes, it only satisfies security concerns for a switched wired network.

3.3 Wireless Firewall Gateways

The past year has seen an adaptation of existing technology to develop a new wireless security solution. Several companies have brought to market what can be best described as wireless firewall gateways (WFG). Baylor University has implemented an in-house WFG based on a NASA whitepaper[1]. The WFG is an all-in-one box that contains a firewall, router, web server, and DHCP server. Tightly integrating all of the services on one box allows for maximum security. First, a user receives an IP address from the DHCP server. Then, the user directs a web browser to the WFG's web server (HTTPS), which requests a username and password from the user. The user submits the request, then PHP executes.

The PHP script attempts to prevent address spoofing and un-authorized network use by comparing DHCP logs with the current ARP table, verifying that the computer that leased the IP is currently requesting authentication with that IP. Authentication credentials are then forwarded to a radius server. Upon approval, the WFG adds rules to the firewall for the requesting IP. Authenticated sessions are terminated upon the expiration of a DHCP lease. During an authenticated session, the WFG verifies that the MAC address leased to a given IP address is the MAC actually using the address. In turn, hijacking an authenticated IP address becomes useless. WFGs adequately cover the authentication and accounting categories of wireless security. Like the previous solutions, the WFG lacks session encryption. While logons are encrypted through as HTTPS session, the remainder of the traffic is left intact as unencrypted.

4. ENCRYPTED SOLUTIONS

In the second category, wireless network security solutions provide encryption.

4.1 WEP

When 802.11b was released, WEP was mistaken as an encryption solution. WEP was only designed to provide *wired-equivalent* privacy on a wireless network. A wireless solution that uses WEP works in conjunction with another security system to provide the authentication and accounting necessary. Even in those situations, WEP does not perform the encryption necessary to consider a wireless network secure. Open source and freeware programs are easily available that crack and decode WEP sessions. Universities provide ideal incubators for such network subversion.

4.2 Virtual Private Networks (VPN)

Some universities have decided to implement virtual private networks to secure their wireless networks, involves installing a VPN concentrator and deploying the VPN client. VPNs were designed with security as the utmost importance. VPNs are able to satisfy all three categories for a secure wireless network.

Authentication and accounting functions are similar to other solutions. VPNs provide a high level of security through their advanced encryption algorithms. The major drawback of VPNs is the requirement of a client. Few manufactures create VPN clients for a wide array of operating systems. As a result, universities deploying this solution may find themselves restricting the supported operating systems for their wireless networks.

5. ON THE HORIZON: 802.1x

Recognizing the flaws in WEP and the necessity to create a new mechanism for network authentication and encryption, IEEE[2] ratified 802.1x standard in the Spring of 2002. "1x" shows promise for improving the security situation on wireless and wired networks. IEEE made the radical but effective decision to push authentication to the edge of the network: under 802.1x, switches and access points act as the gatekeepers to the network. The standard defines a new layer 2 protocol known as Extensible Authentication Protocol (EAP), which creates a framework for transportation of request authentication and encryption information. The framework may then be extended by software and hardware manufactures to facilitate secure authentication and encryption. The resulting solutions have the potential of alleviating security concerns on wireless networks.

5.1 EAP-MD5

The standard also included a baseline version of authentication, EAP-MD5, which presents some interesting issues for secure authentication. Although it is difficult to capture an authentication packet under EAP, a captured EAP-MD5 packet is not difficult to crack. The username is passed in clear text; passwords are encoded using an MD5 hash, then transferred within the packet. As a result, this scheme may be vulnerable to dictionary attacks.

5.2 EAP-LEAP

Cisco was the first vendor to embrace the EAP protocol. Before IEEE ratification, Cisco released their version of 802.1x authentication and encryption. EAP-LEAP was designed to interact with Cisco hardware for the access point and wireless client card. Those requirements have limited the adoption of EAP-LEAP on a wide scale. Recently, Cisco has hinted at the possibility of leaving EAP-LEAP to move to other EAP solutions.

5.3 EAP-TLS

Microsoft[3] quickly followed the 802.1x ratification with their version of EAP. EAP-TLS is based on transport layer security. Client-side configuration is simplified by the inclusion of EAP-TLS in Windows XP (and soon Windows 2000). An enterprise certificate of authority infrastructure is required for implementation. Clients are authenticated through a PKI certificate exchange under the EAP protocol. The certificates may reside on the client computer or on a smart card. While EAP-TLS provides ideal security for a corporate environment, university environments will EAP-TLS implementation difficult. Since student computers are not added to the Windows 2000 domain (in most cases), they do not have the certificates required for authentication. In addition, administration of EAP-TLS on non-standardized hardware may present some difficult challenges.

During the summer of 2002, Microsoft hinted at the expansion of EAP-TLS. They have suggested that MS-CHAPv2 may be included as an authentication mechanism for EAP-TLS. MS-CHAPv2 would result in a more plausible solution for university environments. EAP-TLS has also received a new title: PEAP-TLS, protected extensible authentication protocol transport layer security. The name change is the result of planned inclusion of the 802.11i tumbling WEP keys for encryption. Microsoft plans to release PEAP-TLS as the wireless security solution for the home.

5.3 EAP-TTLS

Funk Software[4] created EAP-TTLS to fill the void in operating system support as well as moving to a secure username/password authentication. Like Microsoft's, the Funk solution is based on transport layer security. The solution does require the installation of client software. While this may seem like a drawback, the client provides robust diagnostic information not yet available under EAP-TTLS. Until widespread operating system support becomes available, client solutions like EAP-TTLS may be the only realistic 802.1x solution for diverse client environments.

5.4 802.11i

IEEE is working on a second standard that will greatly impact the security on wireless networks. 802.11i redefines the standard for encryption on a wireless network. Described as tumbling keys, the standard defines the use of unique WEP keys for short periods of time to foil the ability of cracking the key. 802.11i will transport the WEP keys using the EAP protocol. Once ratified, implementation will require at least an upgrade of firmware on access points and new drivers for clients systems. Many manufactures are anticipating this new standard.

6. CONCLUSION

Wireless networks pose unique challenges for network and security administrators. Close inspection using the three pronged security categories should be completed before ever deploying a wireless network. While few solutions are fully able to pass the authentication, accounting and encryption test, a combination of technologies can provide satisfactory security. In the future, new standards like 802.1x and 802.11i will alleviate many of the present wireless security concerns.

7. REFERENCES

[1]NASA -www.nas.nasa.gov/Groups/Networks/Projects/Wireless
[2]IEEE - www.ieee.org

[3]Microsoft - www.microsoft.com

[4]Funk Software - www.funk.com