International Journal of Smart Sensor and Adhoc Network

Volume 2 | Issue 3 Article 12

April 2012

WIRELESS NETWORK SECURITY THREATS AND THEIR SOLUTIONS: A SHORT STUDY

MADHAVI DHINGRA
ITM College, Gwalior, madhavi0685@gmail.com

DEEPIKA SRIVASTAVA
CSE, Jhansi, deepika.shrivastav3087@gmail.com

VIPUL SHARMA
TCS, Hyderabad, vipul.sharma03@gmail.com

WIRELESS NETWORK SECURITY THREATS AND THEIR SOLUTIONS: A SHORT STUDY

MADHAVI DHINGRA[1], DEEPIKA SRIVASTAVA[2] & VIPUL SHARMA[3]

[1]ITM College, Gwalior, [2]sCSE, Jhansi, [3]TCS, Hyderabad
Email:madhavi0685@gmail.com, deepika.shrivastav3087@gmail.com, vipul.sharma03@gmail.com

Abstract- With continual advances in technology, wireless accessibility is being deployed increasingly in office and public environments, as it is having huge benefits. But it is also coupled with the security threats and risks that will adversely affect the performance of the organization. To get rid of these threats, firstly these threats need to be understood and then their solutions need to be finding out. This paper discusses major security threats and describes their solutions for securing wireless network.

Keywords- *Wireless Network, Wireless Security, Wireless Threats*

I. INTRODUCTION

Wireless networks are becoming more and more popular in homes and offices as they offer a very convenient way to network. Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs.

However, risks are inherent in any wireless technology. Some of these risks are similar to those of wired networks; some are exacerbated by wireless connectivity. Perhaps the most significant source of risks in wireless networks is that the technology's underlying communications medium, the airwave, is open to intruders, making it the logical equivalent of an Ethernet port in the parking lot. The loss of confidentiality and integrity and the threat of denial of service (DoS) attacks are risks typically associated with wireless communications. Unauthorized users may gain access to agency systems and information, corrupt the agency's data, consume network bandwidth, degrade network performance, launch attacks that prevent authorized users from accessing the network, or use agency resources to launch attacks on other networks. An insecure wireless network allows anyone in the vicinity to attach to your wireless network. Once they are on your wireless network they have access to your file servers, databases, email servers, etc.

There are two primary security issues:

- Access - making sure that only authorized people can use the wireless network. Without proper access control anyone in the vicinity of the building can use the wireless network, and thus get access to network.
- Privacy -making sure that no one can watch your communications. Without this, anyone in the vicinity of the building can watch everything you do on a wireless network. This will let them steal your passwords and look at everything you are doing

.

II. SECURITY THREATS

The major threats are as following [1,8,9,10]:
Problem #1: Easy Access
Wireless LANs are easy to find. Strictly speaking, this is not a security threat. All wireless networks need to announce their existence so potential clients can link up and use the services provided by the network. 802.11 requires that networks periodically announce their existence to the world with special frames called Beacons. However, the information needed to join a network is also the information needed to launch an attack on a network. Beacon frames are not processed by any privacy functions, which mean that your 802.11 network and its parameters are available for anybody with an 802.11 card. "War drivers" have used high-gain antennas and software to log the appearance of Beacon frames and associate them with a geographic location using GPS.

Short of moving into heavily-shielded office space that does not allow RF(Radio Frequency) signals to escape, there is no solution for this problem. The best you can do is to mitigate the risk by using strong access control and encryption solutions to prevent a wireless network from being used as an easy entry point into the network. Deploy access points outside firewalls, and protect sensitive traffic with VPNs.
Problem #2: "Rogue" Access Points

Easy access to wireless LANs is coupled with easy deployment. When combined, these two characteristics can cause headaches for network administrators. Any user can run to a nearby computer store, purchase an access point, and connect it to the corporate network without authorization. Many access points are now priced well within the signing authority of even the most junior managers.

Departments may also be able to roll out their own wireless LANs without authorization from the powers that be."Rogue" access points deployed by end users pose great security risks. End users are not security experts, and may not be aware of the risks posed by wireless LANs. Most existing small deployments mapped by war drivers do not enable the security features on products, and many access points have had only minimal changes made to the default settings. It is hard to believe that end users within a large corporation will do much better.

Unfortunately, no good solution exists to this concern. Tools like NetStumbler allow network administrators to wander their building looking for unauthorized access points, but it is expensive to devote time to wandering the building looking for new access points. Monitoring tools will also pick up other access points in the area, which may be a concern if you are sharing a building or a floor with another organization. Their access points may cover part of your floor space, but their access points do not directly compromise your network and are not cause for alarm. The periodic "walk-through" of your campus is the only way to address the threat of unauthorized deployment. At least network analyzers are moving to a handheld form, so you won't have to carry as much.

Problem #3: Unauthorized Use of Service

Several war drivers have published results indicating that a clear majority of access points are put in service with only minimal modifications to their default configuration. Nearly all of the access points running with default configurations have not activated WEP (Wired Equivalent Privacy) or have a default key used by all the vendor's products out of the box. Without WEP, network access is usually there for the taking. Two problems can result from such open access. In addition to bandwidth charges for unauthorized use, legal problems may result. Unauthorized users may not necessarily obey your service provider's terms of service, and it may take only one spammer to cause your ISP to revoke your connectivity. Whether unauthorized use is a problem depends on the objectives of the service. For corporate users extending wired networks, access to wireless networks must be as tightly controlled as for the existing wired network.

Strong authentication is a must before access is granted to the network. If you have deployed a VPN to protect the network from wireless clients, it probably has strong authentication capabilities already built-in. Administrators can also choose to use 802.1x to protect the network from unauthorized users at the logical point of attachment. 802.1x also allows administrators to select an authentication method based on Transport Layer Security (TLS), which can be used to ensure that users attach only to authorized access points. Theft of service was a major concern for connectivity providers in "hot spots" such as hotels and airports. After all, the business model was to charge for network access, so preventing unauthorized access was a business requirement. In the wake of the spectacular failure of some of the former big-name players like MobileStar, the hot-spot connectivity industry is experimenting with new business models. Newer players in the market have based the business model on the idea that free wireless network access is an amenity that might draw guests and convention business. In this newer business model, user authentication is necessary only to ensure accountability. Authentication using a Web browser is a perfectly acceptable solution because it allows sessions to be identified and does not require specialized client software or a certain model of 802.11 network interface.

Problem #4: Service and Performance Constraints

Wireless LANs have limited transmission capacity. Networks based on 802.11b have a bit rate of 11 Mbps, and networks based on the newer 802.11a technology have bit rates up to 54 Mbps. This capacity is shared between all the users associated with an access point. Due to MAC-layer overhead, the actual effective throughput tops out at roughly half of the nominal bit rate. It is not hard to imagine how local area applications might overwhelm such limited capacity, or how an attacker might launch a denial of service attack on the limited resources. Radio capacity can be overwhelmed in several ways. It can be swamped by traffic coming in from the wired network at a rate greater than the radio channel can handle. If an attacker were to launch a ping flood from a Fast Ethernet segment, it could easily overwhelm the capacity of an access point. Depending on the deployment scenario, it might even be possible to overwhelm several access points by using a broadcast address as the destination of the ping flood. Attackers could also inject traffic into the radio network without being attached to a wireless access point. The 802.11 MAC is designed to allow multiple networks to share the same space and radio channel. Attackers wishing to take out the wireless network could send their own traffic on the same radio channel, and the target network would accommodate the new traffic as best it could using the CSMA/CA mechanisms in the standard. Large traffic loads need not be maliciously generated, either, as any network engineer can tell you. Large file transfers or complex client/server systems may transfer large amounts of data over the network to assist users with their jobs. Addressing performance problems starts with monitoring and discovering them. Many access points will report statistics via SNMP, but not with the level of detail required to make sense of end-user performance complaints. Wireless network analyzers can report on the signal quality and network health at a single location, but

tools designed for wireless network administrators are only beginning to emerge.

The initial commercial wireless analyzer offerings were straightforward ports of their wired cousins; new products such as AirMagnet's handheld analyzer look like extremely promising additions to the wireless network engineer's toolkit. No enterprise-class wireless network management system has yet emerged. Some performance complaints could be addressed by deploying a traffic shaper at the point at which a wireless LAN connects to your network backbone. While this will not defend against denial of service attacks, it may help prevent heavy users from monopolizing the radio resources in an area.

Problem #5: MAC Spoofing and Session Hijacking
802.11 networks do not authenticate frames. Every frame has a source address, but there is no guarantee that the station sending the frame actually put the frame "in the air." Just as on traditional Ethernet networks, there is no protection against forgery of frame source addresses. Attackers can use spoofed frames to redirect traffic and corrupt ARP(Address Resolution Protocol) tables. At a much simpler level, attackers can observe the MAC addresses of stations in use on the network and adopt those addresses for malicious transmissions.

To prevent this class of attacks, user authentication mechanisms are being developed for 802.11 networks. By requiring authentication by potential users, unauthorized users can be kept from accessing the network. (Denial of service attacks will still be possible, though, because nothing can keep attackers from having access to the radio layer.)The basis for the user authentication mechanism is the 802.1x standard ratified in June 2001. 802.1x can be used to require user authentication before accessing the network, but additional features are necessary to provide all of the key management functionality wireless networks require. Attackers can use spoofed frames in active attacks as well. In addition to hijacking sessions, attackers can exploit the lack of authentication of access points. Access points are identified by their broadcasts of Beacon frames. Any station that claims to be an access point and broadcasts the right service set identifier (SSID, also commonly called a network name) will appear to be part of an authorized network. Attackers can, however, easily pretend to be an access point because nothing in 802.11 requires an access point to prove it really is an access point. At that point, the attacker could potentially steal credentials and use them to gain access to the network through a man-in-the-middle (MITM) attack. Fortunately, protocols that support mutual authentication are possible with 802.1x. Using methods based on TLS, access points will need to prove their identity before clients provide authentication credentials, and credentials are protected by strong cryptography for transmission over the air. Session hijacking will not be completely solved until the 802.11 MAC adopts per-frame authentication. Until that point, if session hijacking is a concern, you must deploy a cryptographic protocol on top of 802.11 to protect against hijacking.

Problem #6: Traffic Analysis and Eavesdropping
802.11 provides no protection against attacks that passively observe traffic. The main risk is that 802.11 does not provide a way to secure data in transit against eavesdropping. Frame headers are always "in the clear" and are visible to anybody with a wireless network analyzer. Security against eavesdropping was supposed to be provided by the much-maligned Wired Equivalent Privacy specification. A great deal has been written about the flaws in WEP. It protects only the initial association with the network and user data frames. Management and control frames are not encrypted or authenticated by WEP, leaving an attacker wide latitude to disrupt transmissions with spoofed frames. Early WEP implementations are vulnerable to cracking by tools such as AirSnort and WEPCrack, but the latest firmware releases from most vendors eliminate all known attacks. The latest products go one step farther and use key management protocols to change the WEP key every 15 minutes. Even the busiest wireless LAN does not generate enough data for known attacks to recover the key in 15 minutes. Whether you rely on WEP solely, or layer stronger cryptographic solutions on top of it is largely a question of risk management. The latest product releases have no known vulnerabilities. While that is some comfort, the same claim could have been made in July 2001 before release of the current generation of WEP-cracking tools. If your wireless LAN is being used for sensitive data, WEP may very well be insufficient for your needs.

Strong cryptographic solutions like SSH, SSL, and IPSec were designed to transmit data securely over public channels and have proven resistant to attack over many years, and will almost certainly provide a higher level of security.
Problem #7: Higher Level Attacks

Once an attacker gains access to a wireless network, it can serve as a launch point for attacks on other systems. Many networks have a hard outer shell composed of perimeter security devices that are carefully configured and meticulously monitored. Inside the shell, though, is a soft, vulnerable center. Wireless LANs can be deployed quickly if they are directly connected to the vulnerable backbone, but that exposes the network to attack. Depending on the perimeter security in place, it may also expose other networks to attack, and you can bet that you will be quite unpopular if your network is used as a launch pad for attacks on the rest of the world. The solution is straightforward in theory: treat the wireless

network as something outside the security perimeter, but with special access to the inside of the network. Although security diligence is time consuming, so is being sued.

III. SECURING WIRELESS NETWORKS

To secure wireless network, number of points need to be considered that include [2,7,8,9]:

A. Use of Encryption

The most effective way to secure your wireless network from intruders is to encrypt, or scramble, communications over the network. Most wireless routers, access points, and base stations have a built-in encryption mechanism. If your wireless router doesn't have an encryption feature, consider getting one that does. Manufacturers often deliver wireless routers with the encryption feature turned off. You must turn it on.

B. Use anti-virus and anti-spyware software, and a firewall

Computers on a wireless network need the same protections as any computer connected to the Internet. Install anti-virus and anti-spyware software, and keep them up-to-date. If your firewall was shipped in the "off" mode, turn it on.

C. Turn off identifier broadcasting

Most wireless routers have a mechanism called identifier broadcasting. It sends out a signal to any device in the vicinity announcing its presence. You don't need to broadcast this information if the person using the network already knows it is there. Hackers can use identifier broadcasting to home in on vulnerable wireless networks. Disable the identifier broadcasting mechanism if your wireless router allows it.

D. Change the identifier on your router from the default

The identifier for your router is likely to be a standard, default ID assigned by the manufacturer to all hardware of that model. Even if your router is not broadcasting its identifier to the world, hackers know the default IDs and can use them to try to access your network. Change your identifier to something only you know, and remember to configure the same unique ID into your wireless router and your computer so they can communicate. Use a password that's at least 10 characters long: The longer your password, the harder it is for hackers to break.

E. Change your router's pre-set password for administration

The manufacturer of your wireless router probably assigned it a standard default password that allows you to set up and operate the router. Hackers know these default passwords, so change it to something only you know. The longer the password, the tougher it is to crack.

F. Allow only specific computers to access your wireless network

Every computer that is able to communicate with a network is assigned its own unique Media Access Control (MAC) address. Wireless routers usually have a mechanism to allow only devices with particular MAC addresses access to the network. Some hackers have mimicked MAC addresses, so don't rely on this step alone.

G. Turn off your wireless network when you know you won't use it

Hackers cannot access a wireless router when it is shut down. If you turn the router off when you're not using it, you limit the amount of time that it is susceptible to a hack.

H. Training and Educating Users

The importance of training and educating users about secure wireless behavior cannot be overstated. To be effective, user training and education needs to be repeated periodically.

I. Network Auditing

Wireless network auditing is an important part of WLAN security policy. The network needs to be regularly audited for rouge hardware. In this method the network is scanned and mapped for all access points and WLAN nodes. Then this is compared with previous network map. Commonly available network mapping tools like netstumbler and wavelan-tool can be used to do this. Specialized tools such as Airsnort can be used for WEP cracking and auditing the network for weak keys, key reuse and WEP security settings. These methods include the same tests as those carried out by hackers for breaking into the network.

IV. WIRELESS INTRUSION PREVENTION CONCEPTS

Some important concepts for prevention of wireless networks are:

- For closed networks (like home users and organizations) the most common way is to configure access restrictions in the access points. Those restrictions may include encryption and checks on MAC address. Another option is to disable ESSID broadcasting, making the access point difficult for outsiders to detect. Wireless Intrusion Prevention Systems can be used to provide wireless LAN security in this network model.
- For commercial providers, hotspots, and large organizations, the preferred solution is often to have an open and unencrypted, but

completely isolated wireless network. The users will at first have no access to the Internet or to any local network resources. Commercial providers usually forward all web traffic to a captive portal which provides for payment and authorization. Another solution is to require the users to connect securely to a privileged network using VPN.

- Wireless networks are less secure than wired ones; in many offices intruders can easily visit and hook up their own computer to the wired network without problems, gaining access to the network, and it's also often possible for remote intruders to gain access to the network through backdoors like Back Orifice. One general solution may be end-to-end encryption, with independent authentication on all resources that shouldn't be available to the public[5].

There is no ready designed system to prevent from fraudulent usage of wireless communication or to protect data and functions with wirelessly communicating computers and other entities. However there is a system of qualifying the taken measures as a whole according to a common understanding what shall be seen as state of the art. The system of qualifying is an international consensus as specified in ISO/IEC 15408.

Wireless Intrusion Prevention System[WIPS]

A Wireless Intrusion Prevention System (WIPS) is a concept for the most robust way to counteract wireless security risks[3]. However such WIPS does not exist as a ready designed solution to implement as a software package. A WIPS is typically implemented as an overlay to an existing Wireless LAN infrastructure, although it may be deployed standalone to enforce no-wireless policies within an organization. WIPS is considered so important to wireless security that in July 2009, the Payment Card Industry Security Standards Council published wireless guidelines [4] for PCI DSS recommending the use of WIPS to automate wireless scanning and protection for large organizations.

V. INCREASING WIRELESS SECURITY

As discussed, there are some possible means of securing your wireless network beyond WEP. It is unlikely, however, that anyone has a RADIUS server ready and waiting to be used; therefore, you need to identify steps you can take immediately to increase the security of your wireless network. Security-conscious organizations are fortifying their wireless LANs with a layered approach to security that includes the following [6]:

- Putting the wireless network behind its own routed interface so you can shut off access to at a single choke point if necessary
- Discovery of rogue access points and potential associated vulnerabilities
- Physical and logical access point security to ensure that someone cannot walk up to an access point and alter its configuration without your knowledge
- Changing the SSID(Service Set Identifier) and then picking a random SSID that gives away nothing about your company or network
- Disabling active SSID broadcasting
- Rotating your broadcast keys every ten minutes or less
- Encryption and authentication, which might include a virtual private network over wireless
- Using 802.1X for key management and authentication
- Looking over the available EAP(Extensible Authentication Protocol) protocols and deciding which is right for your environment
- Setting the session to time out every ten minutes or less
- Establishing and enforcing wireless network security policies
- Implementing proactive security measures that include intrusion protection

As shown in Figure 1, these steps and recommendations can be illustrated as a phased approach, which enforces the concept of first knowing what the vulnerabilities are and moving forward from that point.

Figure 1.Stages of Securing Your Wireless Network [6]

VI. CONCLUSION

Wireless networking provides numerous opportunities to increase productivity and cut costs. Although it is difficult to totally remove all the threats resulting from wireless networking, it is possible to achieve a reasonable level of security by understanding the threats and then adopting a systematic approach for handling risk. This paper discussed the threats and risks associated with wireless and specified commonly available solutions that could be used for eliminating risks and identify some steps for increasing the security of the wireless network.

REFERENCES

[1] Gast, M. 802.11 Wireless Networks: The Definitive Guide Creating and Administering Wireless Networks, O'Reilley Publishing, April 2002.

[2] Wireless Network Security: Vulnerabilities, Threats and Countermeasures International Journal of Multimedia and Ubiquitous Engineering Vol. 3, No. 3, July, 2008.

[3] PCI Security Standards Council

[4] "PCI DSS Wireless Guidelines". Retrieved 2009-07-16.

[5] "Fitting the WLAN Security pieces together". pcworld.com. Retrieved 2008-10-30.

[6] "Wireless Security". Thomas M. Thomas. Cisco.

[7] Norton, P., and Stockman, M. Peter Norton's Network Security Fundamentals. 2000.

[8] Kennedy, S. (2004). Best practices for wireless network security. Information Systems Control Journal (3).

[9] Wailgum, T. (2004, September 15). Living in wireless denial. CIO Magazine.

[10] Graham, E., Steinbart, P.J. (2006) Wireless Security