Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Wireless Networking: Compromising Security for Convenience?

The Wired Equivalent Privacy (WEP) option to the 802.11 standard is the first step in addressing security concerns; it is an encryption provision. WEP is a security protocol designed to provide a wireless local area network with a level of security and privacy comparable to what is usually expected of a wired network. However since physical security mechanisms no longer apply, the goal of the algorithm is to protect wireless communication from eavesdropping and to prevent unauthorized access to a wireless network throu...

Copyright SANS Institute
Author Retains Full Rights

AD

Wireless Networking: Compromising Security for Convenience?

Kimberly A. Buck
GSEC Practical Assignment Version 1.2f
September 26, 2001

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Wireless Networking: Compromising Security for Convenience?

Wireless Local Area Networks (WLAN)

Wireless networking is becoming increasingly popular for numerous reasons. On the demand side, corporate users are finding wireless networks cheaper and easier to set up and maintain than conventional wired networks. Corporations are also hoping to increase employee productivity by giving employees access to their networks and the Internet during meetings, conferences, and while traveling. Wireless networks are also increasing in homes due to reduced wiring costs and the ability to share broadband Internet connections among multiple computers. On the supply side, the industry is rapidly attaching itself to the dominant technology. As production of wireless products increases, prices are dropping dramatically, speeding up the adoption of the technology on a wide spread basis.

Wireless networks provide all of the features and benefits of traditional local area network technologies such as Ethernet and Token Ring without the limitations of wires and cables. For data transmission, wireless networks utilize either infrared light or radio frequencies. Radio frequencies are more popular for their longer-range, higher-bandwidth, and wider coverage. Wireless LANs typically consist of one or more access points that connect multiple users to a larger Ethernet network or the Internet. PCs or handheld devices equipped with WLAN network interface cards (NICs) are used to link to the access points. The wireless network interface cards are either built in or slide into a PC card slot, leaving a protruding radio antenna.

The Wireless Standard

In June 1997, the IEEE (Institute of Electrical and Electronics Engineers) released the 802.11 standard for wireless local area networking. The standard uses the 2.4 GHz radio band, and allows products with data transmission rates of up to 2 megabits per second (Mbps).

In late 1999, the IEEE approved the subsequent 802.11b, or Wi-Fi standard. This is currently the leading WLAN technology and is supported by more than 80 companies. The standard increased the data processing speed up to 11 Mbps. The Wireless Ethernet Compatibility Alliance (WECA) was founded to promote the adoption of 802.11b WLAN technology and to test and certify equipment for interoperability.

The Wired Equivalent Privacy (WEP) option to the 802.11 standard is the first step in addressing security concerns; it is an encryption provision. WEP is a security protocol designed to provide a wireless local area network with a level of security and privacy comparable to what is usually expected of a wired network. However since physical security mechanisms no longer apply, the goal of the algorithm is to protect wireless communication from eavesdropping and to prevent unauthorized access to a wireless network through the use of encryption. Once WEP has been implemented to protect the data, other typical LAN security measures should be implemented such as password protection and authentication. The WECA has announced that the WEP was never intended to be the sole security mechanism for wireless networks, but when used in conjunction with traditional security measures is found to be very effective.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Current Security Concerns

Just like their wired counterparts, wireless networks face potential security threats each day: unauthorized access to protected network areas; interception from outside; and risks to physical system elements.

Unauthorized network access risks and eavesdropping risks can become an issue because anyone with a wireless data interface can gain access to the wireless cell, and therefore the network. Unlike a wired network where a user must have physical access to a network outlet in order to gain access, access to the wireless cell is available anywhere within the operating radius of the wireless base station. Since WLANs are essentially a shared Ethernet, every member of the wireless cell has potential access to all of the traffic being communicated within the cell. This increases the risk of eavesdropping within a wireless network.

A problem client is another issue related to wireless networking. A problem client is an attached user whose activity interferes in some way with the normal operations of the wireless cell. An example would be a wireless client sending or receiving so much information that it prevents other users from communicating. This could occur intentionally by an inconsiderate user, or unintentionally, by a virus-infected computer for example. Unlike a wired situation, there is no way to disable or identify the location of the offending user. In a wired environment, the activity of each connection can be monitored and controlled.

The inexpensive cost of wireless networking equipment poses yet another threat to the security of wireless networking. A regular laptop installed with a wireless network card can be configured to act as an access point, making it possible for offenders to connect to the network and bypass standard authentication and security mechanisms.

The last major security threat to be discussed is the inadequacy of the WEP algorithm. The WEP algorithm relies on a secret key that is shared between a mobile station and an access point. Packets are encrypted using the secret key before they are sent, and an integrity check is used to ensure that packets were not modified in transit. Three separate research teams have raised questions and concerns about WEP's ability to provide for secure communications. The teams represented colleagues from Intel, University of California at Berkeley, and University of Maryland, College Park.

The research team from Berkeley has given the following explanations of the WEP algorithm and the types of attacks that could undermine the security claims of the technology.

WEP uses the RC4 encryption algorithm known as a stream cipher.

> "A stream cipher operates by expanding a short key into an infinite pseudo-random key stream. The sender XORs the key stream with the plaintext to produce cipher text. The receiver has a copy of the same key, and uses it to generate identical key stream. XORing the key stream with the cipher text yields the original plaintext." (Wagner, p.2)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Operating in this mode makes stream ciphers, and thus the WEP algorithm, vulnerable to several attacks. And although the WEP has defenses against these attacks, the study contends that the measures have been implemented incorrectly, resulting in poor security. Taking advantage of the security flaws, the study was able to mount the following types of attacks using only inexpensive off-the-shelf equipment.

Passive attacks to decrypt traffic

An Initialization Vector (IV) is one of WEP's security defenses. The IV is used to augment the shared secret key and produce a different RC4 key for each packet being sent. Within WEP, the IV is a 24-bit field, sent in the cleartext part of a message. After approximately 5 hours a busy access point will use up all of the IV space, thus allowing a hacker to collect two ciphertexts that are encrypted with the same key stream. From this key stream the hacker can perform statistical analysis to recover the plaintext. Therefore, a passive eavesdropper can intercept all wireless traffic until the key stream is obtained. By XORing two packets that use the same encryption key, the attacker can obtain the XOR of the plaintext messages. The resulting XOR can be used to infer data about the contents of the intercepted messages. The often predictable redundancy of IP traffic can be used to analyze the possibilities of the message contents.

Active attack to inject new traffic

If the exact plaintext for one encrypted message is discovered, the attacker can use this information to construct correct encrypted packets. The counterfeit packet will now be accepted as a valid packet when sent to an access point.

Active attacks to decrypt traffic

Instead of the attacker trying to decipher the content of messages, he may choose to guess about the headers of the packet instead. Typically this information is quite easy to obtain or guess. With the header information, an attacker can flip appropriate bits to change the destination IP address to send the packets to a machine he controls.

Dictionary-building attack

Attackers often have the capability to build a decryption table. Once the plaintext is discovered for a packet, the hacker can compute a key stream generated by the initialization vector used. This key stream can then be used to decrypt all other packets that use the same IV. Over time, the attacker will be able to build a table of IVs and corresponding key streams used to decrypt all packets sent over a wireless link.

The Wireless Ethernet Compatibility Alliance's Response

The WECA acknowledges the research performed by the team at University of California at Berkeley, and admits that the sophisticated methodology they reported is correct. They welcome the report's contribution to raising awareness of wireless LAN security, however, they believe it to be a source of misconception in the media. They issued a formal report to clarify the misconceptions and provide information regarding the state of WEP security. The following is a high-level summary of the WECA's response.

- The WEP is a very effective deterrent against the vast majority of hackers.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- The goal of WEP is to provide an equivalent level of privacy as normally found in an unsecured wire LAN. Wireless LANs have the WEP data encryption where traditional wired LANs have physical security.
- The attacks described in the media are not simple to mount. They would require a high level of sophistication, time, and money.
- A task force has been dedicated to enhancing the security features of WEP. Solutions to the Berkeley deficiencies have been proposed within the latest draft, 802.11e.
- Wi-Fi certified products will be able to implement the security enhancements through firmware upgrades.
- Several vendors already have solutions to the issues described by the Berkeley team.
- The probably of an attack in a home environment is believed to be extremely small, taking into consideration the time and cost of the attack versus the value of the information obtained.
- The biggest security threat to any wireless local area network is the lack of proper security measures, including the implementation of WEP.

Steps For Securing Your Wireless Network

In line with the security threats and vulnerabilities discussed above, Craig Ellison and his colleagues performed a "war driving" expedition that produced some surprising results. During trips on both the west and east costs, 808 networks were surveyed and only 38.9% had WEP enabled on their access points. Luckily for the companies, the group's snooping activities were not malicious in nature. They have simply demonstrated how easy it is for third parties with a notebook computer, an NIC, a $100 antenna and the NetStumbler[1] program to infiltrate wireless networks and possibly gain access to sensitive corporate and personal data. At the very least, hackers could surf the Internet for free through a company's high-speed connection. This study illustrates the need for tighter security measures when utilizing wireless networking capabilities. Craig offers the following suggestions for keeping your wireless network safe.

1. Enable WEP as your first barrier.
2. Change the default SSID (service set identifier or network name) of your product.
3. Don't change the SSID to reflect your company's main names, divisions, or products.
4. Don't change the SSID to your street address.
5. If your access point supports it, disable "broadcast SSID."
6. Change the default password on your access point or wireless router.
7. Locate the access points toward the center of your building, rather than near the windows.
8. Periodically survey your site using a tool like NetStumbler to see if any access points pop up.
9. Take a notebook equipped with NetStumbler and an external antenna outside your office building and see what a hacker parked in your parking lot might see.
10. Consider using an additional level of authentication, such as RADIUS, before you permit an association with your access points.

[1] NetStumbler is a shareware program available on the Internet. When used in conjunction with the proper NIC is "sniffs" for wireless networks.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

11. If using a wireless router, assign static IP addresses for your wireless NICs and turn off DHCP.
12. If you have completed number 11, also consider changing the IP subnet.
13. Don't buy access points or NICs that only support 64-bit WEP.
14. Only purchase access points that have flashable firmware.
15. The most effective strategy for securing your wireless network is to put your wireless access points into a DMZ, and have your wireless users tunnel into your network using a VPN.

Conclusion

Although most technologists continue to write about the inadequate security features of wireless networking, companies are standing strong behind their wireless products and the standard.

3Com Corp.
Tom Werner, Vice President and General Manager
Business Connectivity Group

> "3Com has worked very closely with Microsoft on developing the 802.1x standard and we are excited that Microsoft has adopted it as the Wireless Security standard in Windows XP. The 802.1x standard provides wireless users with a simple and secure form of authentication and authorization that complement 3Com's current security solutions."[2]

Intel Corp
Stephen Saltzman, General Manager, Wireless LAN Operation

> "As wireless networking grows in popularity, customers need to know that confidential information remains private, even as it travels through the air. By working together, the leading companies in this industry have developed a standards-based approach to security that helps protect data without sacrificing the flexibility afforded by wireless mobility."[3]

Cisco Systems Inc.
Bill Rossi, Vice President, Wireless Networking Business Unit

> "As a result of the collaboration between Cisco and Microsoft and our joint development of the 802.1x/EAP standard, enterprises can now deploy a secure, reliable and cost-effective, high-speed wireless networking solution that combines the Cisco infrastructure with the Microsoft Windows XP. This wireless networking security architecture, in use on the Cisco Aironet wireless infrastructure deployed across the Microsoft campus, is the first implementation of the 802.1x draft security

[2] PR Newswire, p. 3
[3] PR Newswire, p. 4

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

standard shipping today, and delivers the complete, end-to-end wireless security that will drive the digital renaissance that Microsoft's wireless strategy prescribes."[4]

© SANS Institute 2001, Author retains full rights

[4] PR Newswire, p. 3

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

References:

Biggs, Maggie. "Unplugged data can also be hack-proof data." Info World. February 26, 2001. URL: http://www.findarticles.com/cf_0/m0IFW/9_23/70888048/print.jhtml (September 23, 2001).

"Wireless Local-Area Networking." January 4, 2001. URL: http://www.cisco.com/warp/public/cc/pd/witc/ao340ap/prodlit/airo_ov.htm (September 23, 2001).

Talley, Brooks. "TEST CENTER RX: Wireless networking looks attractive, but what about the cost of keeping it secure?" Info World. May 22, 2000. URL: http://www.findarticles.com/cf_0/m0IFW/21_22/62241832/print.jhtml (September 23, 2001).

Ellison, Craig. "Exploiting and Protecting 802.11b Wireless Networks." September 4, 2001. URL: http://www.extremetech.com/print_article/0,3428,a%253D13880,00.asp (September 23, 2001).

Arensman, Russ. "CUTTING the CORD." Electronic Business. June 2001. URL: http://www.findarticles.com/cf_0/m0GSY/6_27/75452841/print.jhtml (September 23, 2001).

"Microsoft Galvanizes Industry Effort for Secure Wireless and Wired Local Area Networks." PR Newswire. March 26, 2001. URL: http://www.findarticles.com/cf_0/m4PRN/2001_March_26/72262306/print.jhtml (September 23, 2001).

"Issues with Wireless Networking at CWRU." February 14, 2001. URL: http://cnswww.cns.cwru.edu/net/engr/wireless/issues.html (September 23, 2001).

Wagner, David, Nikita Borisov, and Ian Goldberg. "Security of the WEP algorithm." URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (September 23, 2001).

"Wired Equivalent Privacy." URL: http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci549087,00.html (September 26, 2001).

Wireless Ethernet Compatibility Alliance. "802.11b Wired Equivalent Privacy (WEP) Security" February 19, 2001. URL: http://www.wi-fi.net/pdf/Wi-FiWEPSecurity.pdf (September 26, 2001).

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**