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 Networks: Panacea or the Next Hacker's Playground?

Over the past few years the demand for wireless communications, including wireless networks has grown steadily. Most projections are that the demand will continue to grow in the coming years. Wireless networks offer the potential for changing the way we do networked computing. They also could become the next "hacker's playground" according to a July 19, 2001 article at VNU Business Publications web site. "Although the same rules apply as with securing a wired network, wireless introduces new twists and, because it's a ...

Copyright SANS Institute

Author Retains Full Rights

AD

Wireless Networks: Panacea or the Next Hacker's Playground?

Lee Elmendorf

GSEC Practical Assignment
Version 1.2e
August 15, 2001

Overview

Over the past few years the demand for wireless communications, including wireless networks has grown steadily. Most projections are that the demand will continue to grow in the coming years. Wireless networks offer the potential for changing the way we do networked computing. They also could become the next "hacker's playground" according to a July 19, 2001 article at VNU Business Publications web site. "Although the same rules apply as with securing a wired network, wireless introduces new twists and, because it's a new technology, security is forgotten about. There really isn't any hard and fast way of hardening a wireless network yet," said De Spiegeleire [1]. This paper will provide some background on wireless technology, look at wireless network security issues, then review recent news, and finally offer some suggestions for discouraging the hackers from playing in your wireless backyard.

Background

The physical limitations imposed by wired networks are being swept away by the wireless paradigm. In the short term wireless networks will complement wired networks rather than replace them. This is primarily because wired networks are still cheaper than wireless in most enterprises while also offering greater bandwidth. Additionally, security issues are better known in the more mature wired network environment. Later we'll see that many of the same security measures that help protect confidentiality for wired networks can work in the wireless environment too.

Most wireless networks are based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards with Wired Equivalent Privacy (WEP) for security. The 802.11b products deliver up to 11 Mbps of bandwidth at a frequency of 2.4 GHz, which is comparable to older Ethernet wired networks, but slower than modern 100Mbps switched networks. Access points (also called base stations) transmit their signals in a circular pattern to a maximum range of approximately 300 feet. The upcoming 802.11a standard promises better performance using higher frequencies. One drawback of products using the 802.11b standard is that they share unlicensed frequencies with a host of other products including cordless phones, baby monitors, microwave ovens, and Bluetooth wireless personal area networks. Another drawback of the 802.11b standard is that support for roaming is not specified. This may be corrected by the 802.11f working group that is establishing roaming standards.

As an aside, Bluetooth is a wireless standard that is essentially competing with the 802.11 standards for universal acceptance. L. M. Ericsson from Sweden invented it in 1994. It is named after Harald Blaatand "Bluetooth" II, king of Denmark 940-981A.D. [2]

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

This discussion will focus on security as it pertains to the IEEE 802.11b and WEP standards although many of the same concerns may apply to products based on the Bluetooth standard as well.

Security Issues

Gaining access to a wireless network can be as simple as sitting in the parking lot of the intended target and monitoring their wireless communications. The person standing in your lobby may be checking their personal digital assistant (PDA) for their next appointment or accessing your most sensitive data. As mentioned, the normal range limit of 802.11b is approximately 300 feet but signals can be both transmitted and intercepted from several miles away by using directional antennas. As we will see encryption used in wireless protocols suffers from several flaws, and attack techniques such as denial of service are much easier to carry out on wireless networks.

The hardware to monitor wireless communications is readily available and inexpensive. Although the tools to do actual damage aren't yet readily available, once wireless standards emerge and the technology becomes more widespread, wireless hacking has the potential to become as prevalent as it is on wired networks today.

An ISS white paper on Wireless Networks [3] lists seven known areas of risk with 802.11b wireless technology:

1. Insertion attacks – This involves the deployment of unauthorized clients, PDAs, or access points on the wireless network or creating a new unauthorized wireless network behind perimeter defenses.
2. Interception and unauthorized monitoring of traffic – This is easier on a wireless network since transmissions are across open airwaves and an intruder only needs access to the data stream rather than having to place a monitoring agent on a compromised system as in the case of a wired network.
3. Jamming - Denial of service attacks are easy to accomplish by flooding the 2.4 GHz. frequency. Unintentional jamming may occur if other 802.11b devices are inadvertently added nearby that then degrade the overall signal.
4. Client to client attacks – Clients can talk directly, bypassing access points, so clients need to defend against each other.
5. Brute force attacks on access point passwords – Weak passwords are vulnerable to dictionary attacks.
6. Encryption attacks – Weep if you’re relying on WEP alone to protect the integrity of you wireless network (see below). Known problems with WEP aren’t expected to be addressed before 2002.
7. Misconfiguration - Access points and SNMP agents often ship from hardware vendors not configured or with default passwords that are known to the hacker community.

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

One line of defense against hackers is encryption and as mentioned above, 802.11b wireless networks employ WEP for encryption. WEP uses the RC4 stream cipher to protect data being transmitted. The RC4 stream cipher uses a combination of a public initialization vector (IV) and secret key to create a keystream of pseudorandom bits. The sender XORs the key stream with the plaintext to produce ciphertext. The receiver uses the same IV and secret key to generate the identical keystream. XORing the key stream with the ciphertext yields the original plaintext. Unfortunately the standard version of WEP used in 802.11b is based on a 40-bit key. This is short enough to allow brute force attacks to succeed in breaking the key within a reasonable amount of time.

Another shortcoming of WEP is that the IV used is only 24 bits long and there is no requirement that the IV be changed with every packet. Even on wireless networks where the IV is changed with every packet, heavy traffic will result in a reuse of IV's within a short period of time (often within the same day). This reuse of IV's can make breaking the encryption much easier to accomplish. [4]

Recent News

On July 12, 2001 C|Net news.com reported that "Tim Newsham, a researcher for security firm @Stake, presented the details of weaknesses in the password system of wireless networks that could lead to a break in security in less than 30 seconds. The flaw is the third to be uncovered in the so-called Wired Equivalent Privacy, or WEP, protocol that supposedly secures wireless networks." [5] He went on to say that wireless technology based on 64-bit encryption is insecure and susceptible to being broken in under a minute.

This was confirmed by a study done at UC Berkley by Nikita Borisov, Ian Goldberg, and David Wagner, which found a number of flaws in the WEP algorithm that seriously undermine the security claims of the system. In particular, they found the following types of attacks to be practical:

- Passive attacks to decrypt traffic based on statistical analysis.
- Active attack to inject new traffic from unauthorized mobile stations, based on known plaintext.
- Active attacks to decrypt traffic, based on tricking the access point.
- Dictionary-building attack that, after analysis of about a day's worth of traffic, allows real-time automated decryption of all traffic.

Their conclusion: "We recommend that anyone using an 802.11 wireless network not rely on WEP for security, and employ other security measures to protect their wireless network." [4]

Computerworld reported on July 30, 2001 that Verizon Wireless Inc. and AT&T Wireless have started investigating a security breach that may have allowed outsiders to see confidential information of hundreds of their customers. [6]

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

On August 3, 2001 Reuters reported that researchers had discovered another weakness in Wi-Fi, also known as 802.11b. The new attack allows a hacker to discover the secret key used to encrypt data before it goes into the air. This latest discovery is being treated with more concern than other reports because it is more feasible and takes less time to carry out. A written report that details this vulnerability is being prepared at the time of this paper. [7]

These recent events are the tip of the wireless security iceberg. Existing security vulnerabilities in 802.11b won't be corrected in the near future. More vulnerability will undoubtedly be uncovered in the coming months. Wireless hacking software and hardware will become more sophisticated and accessible. The number of attacks will increase as this technology gains more market share in the coming years. So what's a poor wireless network manager to do?

Solutions

Here are some suggestions for securing your wireless network:

Be sure to include wireless networks as part of your overall network security policy, procedures, and best practices. They need to be subject to all the same rules as wired networks. Extra care should be taken in implementing them since; as we saw above they are even more vulnerable than your wired networks.

Treat your wireless network like the Internet, i.e. it is untrusted. There should be a firewall in place between your wireless network and wired network. That way a successful break-in on the wireless network can't easily penetrate to your entire network.

Your wireless network users need to install personal firewalls on their client systems. This will help limit their vulnerability to attacks from compromised or unauthorized clients.

Some vendors are offering wireless network cards that support 128-bit encryption. As we have seen, the current 40-bit implementation of WEP has already been compromised. Therefore purchasing the more secure 128 bit cards can greatly enhance your wireless security.

Intrusion detection and response sensors must be in place to monitor each segment of the wireless network. Without them it will be impossible to detect the dedicated attacker or even the naïve employee who sets up an access point behind the firewall or other perimeter defenses. This situation is comparable to the problem of somebody placing an unsecured modem on their PC thus bypassing your perimeter and giving dial-in access to your wired network. Run network discoveries on a regular basis to detect any unauthorized access points or clients. You can do this by setting up an agent that monitors the 2.4 GHz frequency looking for 802.11b packets. Check the IP address of these packets to determine which network they are coming from. This could reveal any unauthorized access points that are operating in your area. Note: You could see packets or access points from other organizations if you are operating in a densely populated area.

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

Use a strong password on your access points and check to see if the password is being stored on your clients. Some passwords are stored in clear text in the Windows Registry and are vulnerable to discovery if a client is compromised. Take steps to correct this if possible during your implementation. Every client needs to know the password to communicate through an access point so this gives you many points for a potential loss of security. Change the password on your access points regularly. If very strong security is required then consider having a different password on each access point. That will require users to log on again as they move around, but it will provide an extra layer of security.

Secure shell (ssh) should be used in place of applications such as telnet. Otherwise you are transmitting passwords in plaintext on your wireless network. This same concern applies to wired networks as well. Obviously the strongest password scheme ever devised won't help you if someone can just read it off the wire or airwaves in plaintext.

Virtual Private Networks (VPNs) should be used to augment what 802.11b provides in the way of encryption and authentication. VPNs normally use encryption, user authentication protocols, and tunneling to allow secure end-to-end communications across third party, usually public, networks. In this case your wireless network would be considered the third party network. IP Security (IPSec) protocols are often used in conjunction with VPNs to provide secure communications. IPSec is attractive partly because it can encrypt or authenticate traffic at the IP layer thus making it transparent to the end users, i.e. no training is necessary and it doesn't affect higher layer software including applications. It can be used to secure remote logins, email, client/server communications, file transfers, and Web applications.

Many access points and clients use Simple Network Management Protocol (SNMP) agents that are shipped from the vendor with weak or widely known passwords for both read and write access. If you are running SNMP agents then be sure to use strong passwords in place of the defaults.

Be sure to include your wireless networks in the next security posture assessment (SPA) you run on your wired networks. Of course if you're not already running a regular SPA then you should consider adding it to your arsenal of network defenses. An SPA can help to identify any weak points that intruders could exploit including poorly configured components, weak or missing passwords, unauthorized access points, and the absence of strong encryption protocols.

Conclusions

This paper has provided a brief overview of the IEEE 802.11 wireless network standards. It has also described WEP, the encryption implementation used by 802.11b wireless networks, including many of the known security problems inherent in it. Most experts agree that WEP by itself is not sufficient to safeguard the integrity of your wireless network. We have also seen a few recent news stories that point out the need for enhanced security on wireless networks. Following the suggested solutions presented at the end of

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

this paper will help enhance the security of your wireless network and keep it from becoming the next hacker's playground.

Sources

1. Middleton, James; Wireless networks a 'hacker's playground', July 19, 2001; http://www.vnunet.com/News/1124105
2. Bluetooth tutorial page; http://www.bluetooth.amankansal.com/
3. Internet Security Systems; Wireless LAN Security; http://documents.iss.net/whitepapers/wireless_LAN_security.pdf
4. Borisov N., Goldberg I., Wagner D.; Security of the WEP algorithm; http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
5. Lemos, Robert; Wireless networks wide open to hackers, July 12, 2001; http://news.cnet.com/news/0-1003-200-6554365.html?tag=prntfr
6. Vance, Ashlee; Hack attack targets Verizon, AT&T wireless users, July 30, 2001; http://www.computerworld.com/rckey68/story/0,1199,NAV63_STO62673,00.html
7. Reuters; New weakness found in 802.11 wireless, August 3, 2001; http://www.zdnet.com/zdnn/stories/news/0,4586,5095205,00.html?chkpt=zdhpnews01

© SANS Institute 2001, 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**