

WIRELESS LAN SECURITY

Security
Implications
Of
Wireless
Networking



SECURITY IMPLICATIONS OF WIRELESS NETWORKING

Wireless Security Realized

By Benjamin Harden

The Information Technology Industry has experienced rapid growth in wireless networks over the past few years. The expansion has been fueled by the low cost of deployment and the benefits of enhanced productivity. The biggest problem with this explosive growth is that security has been given a low priority, leaving most wireless networks extremely susceptible to exploitation attacks. This white paper is one of three covering Security, Technologies and Deployment. They were prepared by Datanamics Labs™, to help you assess the technology and determine if wireless is right for you.

“Mistakenly, many organizations believe that their current wireless security policy is strong...”

Mistakenly, many organizations believe that their current wireless security policy is strong enough to protect them from attacks. After all, most vendors promise the security features of Wired Equivalent Privacy (WEP) using 128-bit encryption. This pledge of “Wired Equivalent Privacy” gives organizations a false sense of security. The fact of the matter is that “Wired Equivalent Privacy” is not equivalent to the privacy in a wired network. A hacker can easily scan for wireless Access Points from miles away and decrypt the captured data using easy to find software downloaded from the Internet.

In an effort to address the lack of security with WEP, emerging technologies have promised to fix the issues with the flawed security protocol. However, these new technologies require client side software that is often not available for PDA's because of their weak processing power. Despite the security issues, Wireless Local Area Network (WLAN) installations are on the rise. According to an Allied Business Intelligence report, “In 1999, 1.4 million WLAN devices were shipped worldwide. The number was up to 4.9 million in 2000 and is projected to reach 55.9 million in 2006, representing a \$4.5 billion market.” In an effort to address the security issues with wireless networking, the first step is to identify the vulnerabilities.



“...most novice wireless users neglect to turn on the security features.”

I. Security Vulnerabilities

Wireless networks send radio signals that are not necessarily limited to physical boundaries. Radio signals can go through walls, ceilings, and floors. Therefore, network administrators and decision makers should be aware that there are a number of security vulnerabilities.

Open Wireless LAN

A common yet risky practice of wireless users is a plug-and-play wireless deployment. Although WEP and MAC address filtering are weak security mechanisms and constitute the minimum level of security that a wireless network should have, most vendors have these features turned off by default. Subsequently, most novice wireless users neglect to turn on the security features. War Driving is a name given to the practice of pointing a directional antenna in search of wireless hot spots from a car. In most cases, the hacker is simply looking for an insecure wireless Internet connection that can be used for mischief. Typically, the plug-and-play type deployments are the exact type of “insecure” wireless network for which a hacker is looking. There is even a web site (www.netstumbler.com) that is dedicated to reporting insecure wireless hotspots across North America.

Typically, “hot spots” are easily available because the wireless administrator did not enable any security features. Netstumbler offers a free tool that can be used in conjunction with a laptop and wireless NIC to find and report these hotspots to the public. Regardless of disclaimers that this web site should be a service to inform you if someone has found your wireless network to be accessible to the general public, most of the users of Netstumbler are at best looking for a free Internet connection, or at worst seeking an opportunity for mischief. If your wireless network has been listed in the database then you can ask to have it removed. However, unless you fix the problem, you may find your network in the database again.



" Someone wishing to do malicious harm to your network can slam your wireless frequency with a jamming transmitter..."

Packet capturing and sniffing

An obvious vulnerability of wireless networking is that data is transmitted through the air and accessible to anyone with a receiver. Data can be captured (sniffed) by a number of easily available packet analyzer applications, which can potentially decode the data that is being transmitted. Since a radio wave can be manipulated for strength with any homemade antenna, distance is not always a limitation to the vulnerability of your wireless network.

Denial of Service attack (DoS)


There are many devices that operate in the experimental 2.4Ghz frequency of 802.11b, such as cordless phones, amateur radio, Bluetooth, HomeRF, and even microwave ovens. All of these devices are capable of interfering with your WLAN. Someone wishing to do malicious harm to your network can slam your wireless frequency with a jamming transmitter, which would use up all the radio frequencies in the spectrum and your Wireless Access Point (WAP) would become too busy to respond to valid computers. This type of attack is commonly referred to as a Denial of Service. Imagine for example what kind of damage this would cause at a brokerage firm that was using wireless to transmit time sensitive stock orders.

II. Flawed Security Mechanisms

In an effort to protect the WLAN from an open attack or compromise, the "802.11" standard defines a couple of security mechanisms that can add a limited amount of security to the network. However, both of these security mechanisms are breakable and should be combined with proven security protocols such as IPSec and 802.1x authentication.

MAC access control lists

Every Network Interface Card (NIC) comes with a unique 12-digit Media Access Control (MAC) address that is used in data communications. Every time your computer sends or receives data, your MAC address is used to identify your computer on the local network. With this in mind, it stands to reason that using a MAC address for secure identification of a computer should be sufficient. After all, every NIC comes with a unique MAC address. Many WAPs have the capability to restrict which MAC addresses can use the wireless network. Unfortunately, almost every NIC has the capability to change the MAC



“...a hacker can simply eavesdrop on the network to find out a valid MAC address, and then use the known valid MAC address to reprogram and impersonate the NIC.”


“In a wireless LAN, the network is airborne and is not limited to physical boundaries.”

address to emulate any other MAC address. The problem is that a MAC address can never be encrypted because it must be in clear text for communications on a local network. Due to the necessity of the MAC address being sent in the clear (not encrypted), a hacker can simply eavesdrop on the network to find out a valid MAC address, and then use the known valid MAC address to reprogram and impersonate the NIC. The end result would be that a hacker could easily by-pass the MAC address security list and gain unauthorized access to the network. Hardware based address control is not enough by itself; the hardware should be authenticated with Extensible Authentication Protocol (EAP) identification as described later under 802.1x.

Unlike a wireless network, a wired network has the luxury of a certain level of physical security. In a wireless LAN, the network is airborne and is not limited to physical boundaries. To gain access to a wired network, one would have to connect a cable into the network. This level of security is already in place to the extent that access to the building or offices is controlled. Today's LAN switches have the capability of restricting individual switch ports to a specific MAC address of a valid PC. If a hacker were to gain physical access to a switch port, they would need to know the MAC address that is valid for that specific port. Unlike the example above where the MAC address is broadcast in the air for anyone to eavesdrop, with a wired network, a hacker would have to first gain access to the network before they could listen for MAC addresses. Wireless on the other hand must broadcast a radio signal through the air with the MAC address in the clear. Since radio signals do not necessarily pay attention to the physical boundaries, they are susceptible to interception. Worse yet, a radio signal can be picked up and amplified with a directional antenna. Such is the case with the hacker pointing a homemade “Pringles can” directional antenna into your wireless infrastructure.

Wired Equivalent Privacy (WEP)

WEP is the standard encryption scheme of 802.11b Wireless Local Area Networks. 802.11 WLANs communicate by radio waves that travel between a wireless NIC, usually running on a laptop, and an access point, which is basically a wireless Hub that links wireless users to a wired Ethernet network. WEP uses a highly criticized encryption mechanism that can be compromised because of its lack of a key-management scheme. WEP's encryption process uses a secret key that is intended to



“WEP uses a highly criticized encryption mechanism that can be compromised...”

protect the privacy of the data that is transmitted between the client and the access point by encrypting the data. Utilizing the secret key, the transmitter encrypts data before sending it and the recipient decrypts the data upon receipt. The purpose of WEP is to deny access to the network behind the WAP if the access point and a client do not have the correct mutual WEP key. The most widely used form of WEP keys is the use of static keys. This is due mainly because it does not require any client/server software and is available with almost every 802.11 wireless device. Static WEP keys are like a common password that is programmed into every device on the same WLAN. Since WEP constitutes the major weakness in wireless networking security, we will take a detailed look at the flaws in WEP and how it can be strengthened.

III. More on WEP- The Details of the Attacks

There are two major types of attacks that target the weakness in the WEP protocol. The major difference between the two types of attacks is the time that it takes an attacker to succeed.

Passive Decryption of WEP

In this scenario, a hacker will listen and record the data being transmitted through the air. Occasionally, an Initialization Vector (IV) collision occurs in the data transmissions between the WAP and the clients. An IV is a pseudo-random string that is used to start the encryption process. The IV in WEP is short so there is a mathematical certainty that the same stream will be used more than once resulting in an IV collision. A hacker can use the IV collision vulnerability to find out information about the messages. Typically the information is not exactly clear to the attacker, but a good hacker could take an educated guess as to what has been captured and subsequently use this information to uncover the plain text message. The information from a single IV collision is not always enough to reveal any information. However, a persistent hacker will wait for future collisions of the same IV to further complete the missing piece of the puzzle. This type of attack takes the longest time.

Passive Decryption attack from both sides on WEP

To cut down on the time needed to decrypt messages from the same IV, some hackers could take the passive decryption one step further by sending a message through the wired network to the protected wireless PC and then find out how it is encrypting the known data. If you

“...a hacker will listen and record the data being transmitted through the air.”



“ If you know the original message before the encryption, then you can more easily find out the secret key...”

know the original message before the encryption, then you can more easily find out the secret key for the encryption when comparing the two. A simple example of this can be shown with the coded child’s game “Pig-Latin”. For example, say you captured an encrypted message “llaa eoplepa eemsa ota eedna atada rocessingpa.” At first glance the words do not mean anything. But lets say you knew the original message “ All People Seem To Need Data Processing”, and then you were asked to figure out the key for future messages. You would quickly figure out that the “key” to every word is to move the first letter of each word to the last letter of each word and then added the letter “a”. You could now decipher every future message. Of course the encryption methods in WEP are far more complex, but that is what gigahertz computers and hacker programs are for. In a real scenario, an attacker would be sending known clear text data to the wireless PC from the Internet while monitoring the encrypted version through the air.

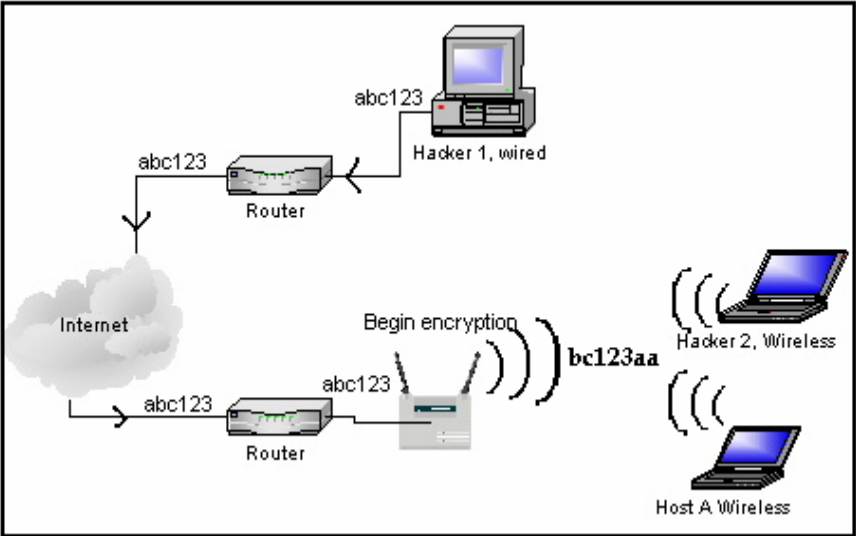


Fig. 1

Message is sent as abc123 through the wired network. The WAP encrypts the data as bc123aa and transmits it on the wired network. Eventually, the hacker is able to figure out the key.





“WEP was never intended to serve as the only means of security on a wireless network.”

IV. A Common Misperception of WEP

According to the IEEE committee, Wired Equivalency Privacy (WEP) was never intended to serve as the only means of security on a wireless network. Instead the IEEE claims, “Just like a wired network, it should be combined with additional security mechanisms such as end-to-end encryption, password protections, authentication, IPSec VPNs, and firewalls.”

It was perhaps the competition for sales by the wireless equipment manufactures that led to the misrepresentation of an all-in-one solid security protocol. For example, Netgear’s Wireless PC card product description boasts, “Standards-based 802.11b technology and 128-bit Wired Equivalent Privacy (WEP) encryption provide your network with the highest level of reliability and privacy”.

V. What’s Next with WEP?

Although the current WEP is not really equivalent to the security of a wired network, the IEEE task group “1” is now working on extensions to WEP, which should resolve the current problems. This future version of the WEP standard is made up of a significant improvement to the authentication methods and an all-new privacy encryption algorithm. Task group “1” is not expected to complete their new WEP standards until 2003.

VI. Security Work-Around with 802.1x

802.1x is a standard that was drafted last year by the IEEE, which will provide the much-needed security to 802.11 wireless networks. Although 802.1x was originally developed for wired networks, it has been proven successful for providing security to wireless networks as well. 802.1x is a port level authentication and encryption protocol that utilizes technologies similar to your typical dial-up-networking connection to an Internet Service Provider. Similar to the MAC access control lists for WAP’s, the port-based security of 802.1x is designed to ensure that only authorized wireless clients can gain access to the network. However, unlike the MAC layer security, 802.1x port based security is far more complex and secure.

“802.1x... has been proven successful for providing security to wireless networks...”





As mentioned in previous sections, the biggest problem with WEP is that it uses the same key for the Initialization Vector when encrypting data. Given enough time, an attacker can figure out the secret key on the network and subsequently gain unauthorized access. 802.1x employs a key management scheme to frequently change the keys without user intervention. An attacker attempting to collect enough data to break a key would become frustrated because by the time the key was figured out, it would have been changed and will be worthless. If you wanted to change your keys without an automatic key management protocol like 802.1x, you would have to manually change the keys on all your wireless devices up to 25 times per day, depending on the amount of traffic on your WLAN.

“If the authentication server said you were authorized, the computer that you dialed up to would permit access to the network.”

The port-based authentication process of the 802.1x protocol can best be described in relation to the familiar dial-up-networking connections to an ISP. If you remember the good old days before Cable Modem and DSL, you actually had to dial up to your ISP through an analog modem. The computer that answered the phone call at the ISP needed to find out your identity by verifying you as a paid customer before allowing you to connect to the Internet. You sent your username and password, which was verified on a centralized authentication server that had your username and password in a database. If the authentication server said you were authorized, the computer that you dialed up to would permit access to the network. The reason for the centralized authentication server is simple; imagine a large ISP like AOL with millions of customers (usernames and passwords) in hundreds of cities and tens of thousands of dial-up servers. Now lets say that Joe12345@aol.com has failed to pay his bill and his account must be disabled. Without centralized authentication, every server would have to be updated to remove Joe12345 from the AOL network. If there were a centralized authentication server, it would only have to be done in one place.

The 802.1x authentication protocol works in a similar way as a dial-up-network, but instead of an ISP authenticating you, a WAP is trying to determine if you are a valid user on the wireless network. 802.1x authenticates you using the Extensible Authentication Protocol (EAP), which supports many authentication mechanisms such as one-time passwords, smart cards, certificates, and others. When you connect your wireless PC (the Supplicant) to a WAP (the Authenticator) that is



“...the authentication is mutual between the authentication server and the wireless PC.”

enabled for 802.1x, your computer starts with an EAP begin message. The WAP will reply back to the wireless PC with an EAP identity request, basically asking, “who goes there”? The wireless PC will respond with the identification for the network. The WAP, which does not know anything about identifications, will forward the EAP authentication to a centralized Authentication Server (AS) to find out if your PC is allowed on the network. The Authentication Server will lookup your identification and respond to the WAP with a “reject” or “accept” message.

It is important to know that the authentication is mutual between the authentication server and the wireless PC. The PC will verify that the authentication server is not a rogue server, and the authentication server will verify that the PC is valid for the network. The WAP will subsequently forward the “accept or reject” message to the PC. If the authentication is mutually accepted, the Authentication Server and the PC will dynamically derive WEP keys for data encryption between the WAP and the PC. The authentication server will send a newly created key over the wired portion of the network to the WAP. The key that is sent over the wireless network to the PC will be encrypted using a shared secret session key, which is mutually known between the radius server and client PC. The WAP and the PC will activate WEP and begin to transmit encrypted data utilizing the dynamic keys. At a predetermined interval (the default is 60 min.), the PC and authentication server will derive new keys to help prevent a passive attack.

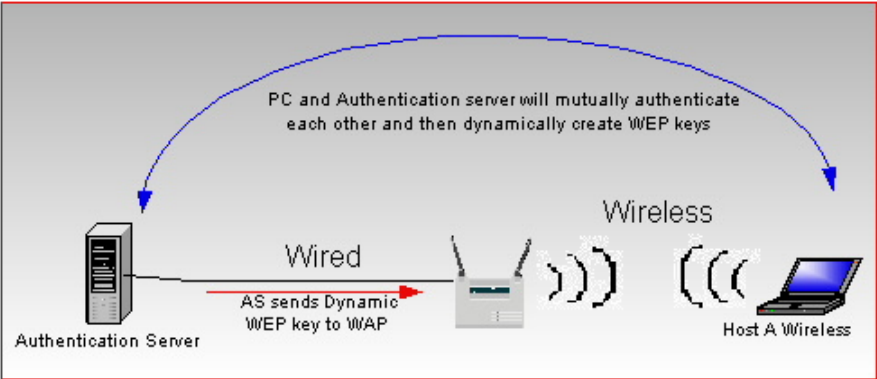


Fig 2 802.1x and EAP

A problem with the deployment of 802.1x is that it requires client side software to be installed on all the wireless devices in a network. A large-scale deployment of such software becomes an administrative issue





as standards and versions must be maintained. Microsoft Windows XP comes equipped with the 802.1x protocol and many vendors now offer 802.1x as an add-on product for your older operating system. Cisco has been offering a proprietary version of EAP (called LEAP) and 802.1x since late 2000.

VII. Rogue WAP- Another Wireless Security Issue

The rogue WAP installation is an additional way that a wireless device can be used to compromise the security of a wired network. Even if the design of your network does not include WLAN equipment, a hacker could place a rogue WAP on your network. It is important to understand how your network could be at risk and how to stay protected.

Access points are useful tools for hackers to break into a network. For example, your IT department feels good about the security of the network; they have put in place the best firewalls money can buy, protecting them from the distrusted Internet community. However, if a hacker gains physical access to the network and implants a small WAP in a discreet location in the building, the hacker could potentially use this WAP to gain access to your network from a car located in the parking lot. This scenario is not only physically possible but it is financially feasible with a low profile, low cost WAP. Today's access points have been getting smaller and less expensive than the early WAPs of 802.11, they can be found at most computer stores starting at \$99.

“...the hacker could potentially use this WAP to gain access to your network from the parking lot.”

This same security issue can become a problem when an employee unknowingly puts the company network at risk by installing an unauthorized WAP on the network. A rogue WAP can be installed on your network by an employee with good intentions and be used by a hacker with malicious intent. For example, a user at ABC Corp has been using wireless at home for some time now. To solve a physical cable limitation at the office, the user has brought in a WAP from home and plugged it in to a company Ethernet connection. The user is proud because it is now possible to be twice as productive. After defeating a physical limitation, the user now has two network connections, one for the company PC and one for the wireless laptop. Unfortunately, the user did not change the WAP from the default settings of no security. What the user has done is bypassed the company firewall and advertised the company network to anyone with an antenna. A “war-driver” may notice



“A rogue WAP can be installed on your network by an employee with good intentions...”

this wide-open hotspot at ABC Corp and list it on Netstumbler.com for anyone in the area to enjoy. This situation could also be a problem when a telecommuter uses a home WAP that is connected to the company VPN. Although the user can work more comfortably with a wireless laptop when receiving data from the company, so can the next-door neighbor.

You can substantially reduce the possibility of a rogue WAP installation on your network by using the same tools that the hackers use. For example, you could use Netstumbler to actively monitor your network for advertising WAP's. Once you have detected the rogue WAP, you could use the available signal strength utilities to locate and disable it.

VIII. Summary

“Security should always be the number one priority for any technology...”

Wireless networking is growing at an astounding pace. When a new technology like wireless is expanding rapidly, the security aspect is often overlooked for a good return on investment. Security should always be the number one priority for any technology as a compromise of security can be devastating. Although the initial attempts to secure 802.11 proved to be weak, emerging technologies are providing valid solutions, both temporary and permanent. 2002 and 2003 should be interesting years for the maturity of security in a technology that promises real improvements in productivity and a good return on investment.



4045 South Spencer Street
Suite B - 38
Las Vegas, Nevada 89119
www.DatanamicsInc.com
Voice | 702-697-2263
Fax | 702-697-2299
E-Mail | Info@DatanamicsInc.com

