

Basic Security Mechanisms for Wireless Networks

Joe Klemencic 2001-07-16

Basic Security Mechanisms for Wireless Networks

by Joe Klemencic

last updated July 16, 2001

As more companies start to deploy wireless networking, important security aspects are often overlooked. Wireless networking was initially marketed towards home consumers and specialized applications, but was limited by low throughput speeds. As the technology matured, networking standards were introduced to ensure interoperability between vendors, and greater speeds were obtained. Driven by both the demands of the users and the flexibility offered by wireless networks, businesses started to deploy wireless networks in areas that were difficult to provide wired-based networking topologies, such as warehouses and conference rooms. Unfortunately, due to the ease of wireless deployment, and the freshness of the technology, many network engineers do not realize the risks associated with operating a wireless network. Even if proper precautions are taken to ensure a secure wireless network environment, there is still the risk of a user purchasing their own wireless Access Point (AP) or base stations and installing it on the network unbeknownst to the IT staff.

What Exactly is a Wireless Network?

Historically, communications between computer systems have been tethered together with cables and wires, but that is rapidly changing. Wireless networks offer communication between computer devices almost anywhere, unconstrained by the physical limitations of a wired network. Before we get started, there are a few primary components that make up a wireless network you should be familiar with:

- Wireless Access Points (AP) which provide connectivity between traditional wired networks and the unwired world;
- Wireless Network Interface Cards (wNIC) installed in computers to access the Wireless Network; and,
- The Wireless Local Area Network (wLAN) itself containing a combination of AP's and wNIC's.

In a typical wired network, a computer is connected to other computers via a cable of some

type. Electrical pulses or optical light waves carry data from the computer to the networking infrastructure equipment where it is then carried to the final destination via even more cables. In a wireless network, this same data is instead transmitted over the air in radio frequencies, similar to the operation of cellular phones. A computer wishing to talk on a wireless network must first connect, or associate, to a wireless Access Point. This association is similar to plugging a network cable into a computer on your desk. If no mechanism exists on the wireless network to identify or authenticate the computer attempting to communicate on the wireless network, data communication is freely established.

Since wireless networking is simply a new method of transporting data without wires, applications such as e-mail, web browsing and sharing of data files can continue to operate uninhibited. Furthermore, many specialized variations of wireless network technologies are starting to merge together to provide seamless resource connectivity and sharing, which reduces implementation and operational costs. Portable hand-held barcode scanners that traditionally operated on their own proprietary architectures now operate on standard Ethernet networks and infrastructure. Personal electronic organizers can now automatically update contact and calendar entries and even surf the web from almost anywhere. There have even been tests in some grocery stores to automatically update a digital price tag for displayed products without actually having to physically visit the shelf. As you can imagine, with the number of vendors and applications vying for a niche in the marketplace, a wide variety of disparate systems and services have arisen. The need for some sort of standardization quickly became apparent.

In order to facilitate a standard mechanism for otherwise incompatible wireless services to interoperate, the [Institute of Electrical and Electronics Engineers \(IEEE\)](#) formed a committee to extend the standards established for Ethernet communication to the Wireless network. This standardization allows for any wireless device to now operate on an Ethernet network just as a personal computer does. Without a method to restrict access to only authorized devices and users, an entire network can easily be compromised given the free and open connectivity of Wireless networking, and can be done without ever obtaining physical access to the network itself. One can now quickly and easily install a wireless network in a home or office with little or no networking knowledge for as little as \$300. However, the convenience and availability of these wireless networks comes at a cost - they may pose a security risk.

Why are Wireless Networks at Risk?

As the name implies, wireless networks provide network connectivity in a wire-free environment. While the freedom from physical constraints of a wired environment can be greatly liberating, it also means that the information being communicated along the network is free of physical constraints, this can create problems in controlling who is able to receive the data. Wireless networking allows for network connectivity in large areas where running physical cabling is not practical, such as in a large distribution warehouse, in dynamic areas such as conference rooms where an undetermined amount of users require network access, or to allow for ease of use for roaming users, such as an administrator wandering from computer room to computer room. While wireless networking provides great flexibility, it does not simply stop at the building walls. The wireless signal currently can be detected up to 1500 ft. away, and at even greater distances with specialized equipment.

A plan designed to allow wireless connectivity to a conference room may also have enabled network connectivity in the parking lot or possibly to another company on another floor. Unauthorized users could easily purchase a wireless network interface card and connect to a network, thus completely bypassing firewalls or other protection mechanisms. This could allow the malicious user to sniff passwords, steal proprietary information, launch untraceable denial of service attacks or hack another company with the target companies' resources, which could leave the company open to legal recourse or public humiliation. Attempts to track down the attacker will be difficult, if not impossible.

How Can Wireless Networks Be Compromised?

In the not too distant past, inquisitive computer users utilized a technique called 'war dialing' to identify potentially vulnerable systems. War dialing is a process in which computers sequentially dial ranges of phone numbers, logging any phone numbers that successfully connected to a computer that responds. The malicious users would then browse their log files and initiate directed hacking attacks at the computers that were found to respond. With the introduction of wireless networking, malicious users may now hit the streets in their vehicles to perform 'war driving' to discover vulnerable wireless networks. War driving is the practice of walking or driving around business complex or a neighborhood with a wireless-enabled laptop computer, connecting to and mapping any number of corporate and private networks. This essentially gives the war driving hacker access to those resources with the same privilege as one of their employees, all while remaining undetected. Directed antennas and special amplifiers connected to the attackers' computer allow for connectivity at much greater distances, so that they are not necessarily restricted to prowling around parking lots or circling the block continually (not to

mention suspiciously.) For a more in-depth examination of war dialing, please see [War Driving by the Bay](#) by SecurityFocus journalist Kevin Poulsen.

Another common technique is for an attacker to 'camp out' at a public wireless implementation, such as an airport. There, an unsuspecting business traveler may decide to check his email and transfer expense reports back to the home office while waiting for a flight. The attacker waits patiently, and captures every packet transmitted from the traveler's computer. In this way, an attacker may obtain passwords that would allow unauthorized access to a network, credit card information and possibly even proprietary information.

These unauthorized access attempts do not generally require any special software or special skills. In most cases, troubleshooting software provided by the vendor of wireless network cards is usually sufficient. This bundled software ranges in function, but most allow measurements of signal strength of a Wireless connection, which translates into how fast their connection is, and can indicate how far away the workstation is from the wireless base station. Many vendors now offer packet capture applications for use on wireless networks, very similar to the network packet capture utilities used by thousands of IT professionals to troubleshoot network connectivity and performance problems. These applications offer the ability to capture every bit of data that traverses the airways for later inspection.

How to Protect the Wireless Network

Many different methods to secure wireless networks exist today, each with their own caveats, while more are emerging over the horizon.

Explicit Client Restrictions

Typically, the Ethernet address, or MAC address, of the users' wireless network interface card can be programmed into a wireless Access Point to allow access only from specific network interface cards. This mechanism is handy for a small wireless installation, where specific wireless network interface cards can be distributed to users for an event, such as a meeting in a conference or home installations. However, this method can quickly create enormous administration overhead, for the individual interface cards must be tracked, and the addresses of these cards must be programmed into each wireless Access Point where access is desired. Although this technique restricts access to only a few network cards, a crafty intruder could reprogram their wireless network interface card with an allowed address and gain access to the

wireless network.

User Authentication

Many vendors offer custom user authentication mechanisms before granting access to a wireless network. Typically, a username and password is created on the wireless Access Points, and a custom application is installed on the users' computer. The user must first login to the network via this application before they can connect to the wireless network. Administration tasks for this solution is fairly high, for the users login must appear in every wireless Access Point where access is desired, and yet another password must be remembered by the user.

This authentication method provides a certain level of security, but is not without risks and caveats. In most cases, the user may set this password to the same password used for access to other systems, which would jeopardize other computing resources if the password were compromised. Depending on the method used to send the password to the wireless Access Point, an attacker could capture the login sequence 'out of thin air', or possibly launch a brute-force password crack against the wireless Access Point, which essentially tries to continuously login by trying various password combinations until it "cracks" the password. This vendor-specific authentication method may also restrict the types of clients that can connect to the wireless network. Typically, vendors only provide Microsoft Windows clients, while overlooking other platforms.

Network Naming

As the wireless networking technologies matured, a standard known as Network Naming was developed to provide a level of secure access. A Network Name, or SSID, may be assigned to a wireless network, and programmed into each wireless client. This Network Name is first verified when a wireless client attempts to connect to a wireless Access Point. If the name does not match, connectivity is rejected. Some administration responsibilities are required to program the Network Name into each wireless client upon the initial installation, and every time the Network Name is changed. Since this Network Name can be viewed in the clients network properties, and is transmitted over the wireless network in unencrypted form, an attacker can obtain it with little effort.

Wired Equivalent Privacy (WEP)

Recently, a method to encrypt the wireless data was introduced. Wired Equivalent Privacy (WEP) offers the ability to encrypt data utilizing either 40-bit or 128-bit encryption algorithms. The current WEP implementation utilizes a shared-key method, in which a 'password' is created and installed on every wireless device and wireless Access Point. Data communications are encrypted and decrypted with this key. Attackers cannot easily obtain this key through packet capturing techniques, but instead rely on brute-force cracking of capture data streams, or other social-engineering methods. If this encryption key is compromised, an effort must be made to create a new encryption key and to configure each wireless client with the new key. It has recently been discovered that WEP is vulnerable to various attacks and reverse engineering of the encryption keys utilized. Readers can learn more about this problem in [Security of the WEP Algorithm](#) by Nikita Borisov, Ian Goldberg, and David Wagner.

Emerging Standards

The IEEE has identified problems with each of the currently available wireless security mechanism. It has been working on documents to mitigate the risks and administration overhead associated with each technique, while ensuring operability with the majority of Wireless clients. These documents are the 802.11x and 802.11e standards. These documents discuss the ability to provide user-level authentication against popular authentication mechanisms utilized for Remote Access methods. Current wireless vendors are starting to adopt the methods described in these documents, and should be releasing products that utilize these methods later this year.

Firewalls/VPN

In a large wireless implementation, a firewall approach may be desired. Instead of having to create and maintain separate wireless authentication mechanisms, the wireless networks may be treated as one would treat access to the Internet. The wireless network could be separated from the corporate network with a firewall, and existing VPN technologies could be used to gain access to business resources. The firewall is configured to only allow VPN connections from the wireless network to the VPN server, and the VPN server may provide encrypted transport of the wireless data from the client. No special authentication mechanisms are needed if an existing VPN solution is currently installed. With this technique, users may already be used to using the VPN software for remote access, and will thus be familiar with the restrictions imposed by using the VPN. This will help to ensure a seamless transition to the security imposed on the wireless network.

What can be done now

If readers have a current wireless installation, or are planning on installing wireless soon, the architecture should be reviewed to ensure adequate security mechanisms are in place. The wireless Access Points should be secured physically and logically, much like networking switches and routers are. If possible, general user access to the Access Point configuration should be restricted by changing the Access Point passwords, SNMP community names and utilizing access controls. Current data security policies should be reviewed, and clause to prohibit users from installing their own wireless Access Points without prior IT knowledge should be added. The networking and administration staff should be trained in the operation of wireless technologies. Evaluate current remote access methods and determine what can be adapted to the wireless network. Query your wireless vendors for information and support of the emerging IEEE 802.11x standards. Consult your product documentation to determine if a method to decrease the wireless Access Point signal strength is available, which will limit the distance in which connectivity to the wireless network is established. Choose a few appropriate security mechanisms from the methods currently available, with regards to the wireless implementation size, administration staff available and acceptable risks to be assumed. Above all, try to provide a seamless security mechanism to allow authorized users to connect to the wireless network while making it difficult or impossible for unauthorized users.

Looking to the Future

Wireless networking is still in its infancy stages. The IEEE has formed [Wireless Committees](#) to recommend interoperability and security standards. Most wireless vendors are starting to include support for these developing standards in their wireless product lines, and networking equipment vendors are also developing solutions to provide user authentication before gaining access to network resources. As the technology matures, more techniques will become available. One possible solution currently being investigated is to integrate VPN-type technologies directly into the wireless clients and base stations. Wireless network bandwidth is also increasing, with speeds in the 20MBs and 50MBs ranges just over the horizon. Prices are also starting to fall, allowing for affordable wireless connectivity to reach outside of the corporate environment and into people's homes. Several Internet providers are testing broadband wireless connectivity in select regions to compete against other broadband offerings such as DSL and Cable Modems. As wireless networking becomes commonplace, the issues discussed in this article will become more prevalent and more urgent. As the use of wireless

technology increases, everyone will need to become security conscious: users, administrators and vendors.

Joe Klemencic is currently performing Data Security responsibilities at Fermi National Accelerator Laboratory in Batavia, Illinois. He has spent the past 10 years in network architecture support, design and security.

Relevant Links

[802.11 Wireless Local Area Networks](#)

Institute of Electrical and Electronics Engineers (IEEE)

[Security of the WEP algorithm](#)

Nikita Borisov, Ian Goldberg, and David Wagner, Berkeley

[Wireless LAN Security](#)

Cisco Systems, Inc.

[WLANA Security](#)

Enterasys Networks

[Privacy Statement](#)

Copyright 2006, SecurityFocus