Security of Wireless Networks and Mobile Devices

Abstract

As the need for security on any network is apparent, the prevention of eavesdropping and the desire for authentication has been the main focus of many network administrators. However, the problems that already exist are added to when you add wireless networking to the equation. As wireless networking becomes more popular, the flawed security of most of those networks, amplified by inability to physically protect the media, becomes more apparent.

Several organizations have devised ways to secure their wireless networks from intruders. However, there is currently no wireless security implementation that everyone agrees is always suitable, regardless of what network it is to be used on. Some implementations are satisfactory for some environments, and there is work underway to create future solutions. Meanwhile, some wireless users make the situation more difficult as they advertise existing vulnerable networks.

Eavesdropping and Authentication

When considering a network with a Wireless Access Point, or “WAP”, available, new security concerns come into play. Because wireless is broadcast in nature, anyone within range of a wireless card can intercept the packets being sent out without interrupting the flow of data between wireless card and base station.

It is because of this that wireless network security is somewhat more concentrated than that of wired networks. Network administrators with WAP’s tend to focus on the security between the wireless card and the base station. After packets leave the base station on the wired side, administrators can rely on more conventional security features already in place on their wired networks to protect the information in question.

There are two main issues that wireless security solutions tend to address. First, since all wireless packets are available to anyone who listens, security is needed to prevent eavesdropping. Since it is impossible to physically keep people away from the WAP’s, short of erecting a fence around your building, solutions tend to rely on encryption in one form or another. Depending on what is implemented, this can include a static shared key, a key generated from a static key, a dynamically-generated key, or negotiated keys.

The second issue is authentication. With a wired network, a system administrator might determine who generated certain traffic based on the physical port that the traffic came in on. By assuming that inbound traffic on a particular port is always coming from a certain source, there is no need to constantly verify where the traffic was coming from. However, with wireless networking, many users can access the network at the same access point, making it more difficult to map who did what. It is often desirable, therefore, to allow users to identify who they are before letting them through the base station onto the rest of the network. This prevents unauthorized usage while having the added bonus of being able to track a particular user’s activity should the need arise.

When considering a security solution for your wireless network, it is important to keep these issues in mind. However, for various reasons, it isn’t always possible to get a total solution for a particular network.

WEP and the Small Network

The idea of a no-wires network is becoming more appealing to home and small office users every day. The cost of such connectivity, as opposed to paying someone to install Category 5e cable in your house wherever you think you might want to use your laptop, is decreasing every day. “With the huge volume of cards being offered by close to 100 vendors, prices have plummeted to sub-$100 for notebook cards, and as low as $150 for access points.”1[1] Bandwidth is also becoming less of an issue. 2.4GHz 802.11b wireless can provide 11Mbps of data, while 5GHz 802.11a wireless, for an added price, can provide up to 54 Mbps, more than enough to take full advantage of a cable modem or DSL connection.

In terms of security, it is these ad-hoc networks which most often provide the easiest access to outsiders. The main problem here is the cost of security. A large company with a large number of people using the network can afford to purchase appropriate security equipment, and to pay someone to secure their network and maintain that security. A home or small office user, on the other hand, will most often rely on inexpensive security measures. A $6.000 wireless security gateway and a RADIUS server, for example would not be cost-effective for a small office.

More often than not, the small-network wireless user will utilize only whatever security features are advertised on the box of the wireless products they purchase. Because it is part of the 802.11 specification, a security feature known as Wired Equivalent Privacy (WEP), is available with most base stations sold today. An encrypted key is associated with each network; anyone who wants to use the network must have that key. Many people rely on WEP to prevent their packets from being sniffed and to prevent outsiders from joining their network without their knowledge.

However, WEP is by no means secure. An experienced wireless hacker has a wide variety of attacks with which to circumvent WEP. In most cases, this involves listening in on broadcasted wireless packets and breaking the encryption key. Statistical attacks become increasing practical as more ciphertexts that use the same key stream are known. Insufficient number of possible keys and "man-in-the-middle" attacks make the situation even worse.

One of many free programs available to accomplish this is AirSnort. AirSnort requires approximately 5-10 million encrypted packets to be gathered. Once enough packets have been gathered, it can guess the encryption password in under a second. Once that is accomplished, it is no trouble to join the network in question.

WEP also falls short in other areas. The use of WEP can have a significant impact on your throughput, as opposed to having no such encryption. Most generally-available wireless hardware loses significant bandwidth (up to 40%, in some tests) when encrypting traffic in hardware. In addition, because each network shares a single encrypted key, you are only protecting your network from an outsider from eavesdropping on your network, not users from listening in on each other.

Larger Wireless Environments

Putting aside the fact that WEP is not as secure as it claims to be, it is currently unsuitable for larger environments. Most system administrators prefer authentication schemes which allow them to determine which users were doing what at a certain time. It is also often desirable to allow users to be independently protected from one another with unique, separate encryption keys. There are a number of security implementations beyond WEP which try to solve these problems, although some network administrators would prefer less or no security.

Some network administrators can't be bothered with the expense and the work required to monitor their network from intruders. If given a choice between having a network up with no security or not having a network up at all, they would chose the former. An example of such an environment is Columbia University's Wireless Network. Essentially, anyone can configure their wireless card for DHCP, put their wireless device within range of a base station, and start using Columbia's network services. They have no way to track someone engaging in illegal activities on their network; while MAC addresses might be logged, those addresses are not mapped to any kind of user identification. Some Internet cafés and airports also allow such service for their customers, although more of these networks are implementing security measures.

Some organizations use static addressing for their security. Users are assigned a static IP by a central authority. Since it's easy enough to change your IP to use someone else's, that central authority might also log MAC addresses of users' wireless cards. A security mechanism residing at the base stations or at the firewall checks to see if a MAC address being used is associated with the static IP assigned to that address. If there is a match, traffic is free to pass through onto the network; otherwise, it is rejected.

A similar concept is the use of a DHCP reservation. Again, a central authority is responsible for keeping track of MAC addresses. When your MAC address is seen on the network, you are either granted or denied an IP via DHCP. The IP can be assigned only for use by you, or can come from a reserved pool of addresses.

The use of both these methods is generally not viewed as acceptable methods of authentication. For one thing, it is little trouble for someone to listen for your wireless traffic, pick up your IP address, and pretend to be you. With little additional effort, the MAC address of many wireless cards can be changed. An intruder can learn your MAC address from your transmissions, change their address to match yours, and get an IP whenever they wish. In addition, neither of these methods does anything to solve the problem of preventing eavesdropping.

Another method of wireless authentication, developed by Rutgers University's Department of Computer and Information Sciences, is known as "Archipelago Wireless". Archipelago Wireless offers authentication before you get to connect to anything. All base stations route requests through a central firewall which sits between the base stations and the rest of the network. Users open a browser and go to the network's login page; attempts to open any other page are re-directed to the login page, while other connections are denied. Once on the SSL-protected login site, users are given the opportunity to authenticate against a RADIUS server. If authentication is successful, their traffic is allowed to pass through to the rest of the network. The firewall queries their wireless card every few minutes to make sure that the connection is still alive.

The concept used by the Wireless Archipelago is almost identical to what is being implemented by T-Mobile Hotspot, a service to be installed in 1,200 coffee shops owned by the Starbucks Corporation by the end of 2002. For a small fee – "…an unlimited-use account in one city costs $29.99 a month…" – users can connect when within

range of an equipped shop. While the DCIS's goal was to make the network available to those with appropriate access, Starbucks is primarily interested with having registration and accountability for billing purposes.

While the problem of accountability has been well addressed by Archipelago Wireless, it does not address the problem of eavesdropping prevention. However, networks with this type of setup are designed to with other security features, not to replace them. The use of SSH for login sessions and SSL for email reading is recommended, while the use of a VPN is possible for protecting all traffic.

VPN servers can be configured to use their existing methods to implement authentication. Relying on a VPN for wireless security, however, has its own problems. For starters, you have to have a way to deploy the appropriate VPN client to your users. While it might be possible to post connection information around campus, it would be a bit more difficult and more costly to have boxes with VPN client CD's. You might make this client software available on your network web site, but users would have to be on the network to download it. Second, the VPN client you chose may not be compatible with or available for all operating systems used by those who wish to access your network. This problem becomes less apparent in a homogeneous environment, such as a corporation, where system administrators can expect their users to only have certain kinds of wireless devices. There is also the issue of VPN's being a drain on bandwidth.

Bluesocket, Inc., offers a solution which is a combination of Archipelago Wireless and VPN server in one box. Their gateways similarly ask users to authenticate on a login page, which can be directed to call upon a secondary authentication server. In addition, Bluesocket adds VPN security over IPSec, a security protocol considered by most to be more secure than WEP. While not all operating systems have compatible IPSec clients built in or available, the number of operating systems that do have IPSec is going up. Bluesocket's security does come at a price: a firewall for 100 users costs around $6000.

Cisco's Aironet wireless cards and base stations take advantage of a number of security features which answer a lot of authentication and encryption questions. Aironet uses an authentication scheme based on Extensible Authentication Protocol (EAP). Known as EAP-Cisco Wireless, or "LEAP," this scheme "provides user-based authentication and centralized key management and distribution." First, the user enters their username and password into the client adaptor. This information is sent from the WAP to a compatible RADIUS server for authentication. The server and client then negotiate a dynamic, session-based WEP key based on a one-way hash of a known secret. This key is set to expire a regular intervals, making it harder for sniffers to discover the key before it becomes invalid. While few non-Cisco products currently take advantage of LEAP, Apple's AirPort base stations and wireless cards are compatible.

War Driving and War Chalking

As wireless networking becomes increasingly popular, more and more people are looking for places they can pick up wireless Internet access. As was mentioned earlier, wireless networking is broadcast in nature, which means that wireless transmissions can be picked up by anyone within range of a base station, whether the owner of that base station knows about them or not. Once this was realized, wireless owners started a trend known as "war driving", the ongoing search for vulnerable access points where they might plug in and access unsecured networks.

"War driving is the updated version of 'war dialing' – popularized in the 1980's by the movie *War Games* – in which a PC dials number after number attempting to locate other modems." The idea behind war driving is similar: find out what networks are available to you and then attempt to access them.

War driving primarily involves driving around with suitable antennae and software and looking for vulnerable access points. There are a surprisingly large number of web sites that will identify the software necessary and give explanations on how to do this. Free software, such as NetStumbler, is designed to pick up wireless networks. Once a wireless signal is identified, NetStumbler logs all available information one might need to get into that network later. Although war driving can be successfully accomplished with an out-of-the-box wireless card and little else, a more enthusiastic war driver can learn how to purchase and install a bigger, more sophisticated antennae to pick up more signals. It is also common for war drivers to bring along GPS equipment to map their findings for later use.

Once you find an access point, it is then little trouble to join that network. Using NetStumbler combined with a program such as AirSnort, it is not difficult for any war dialer to compromise any wireless network using either no security or only WEP security. As mentioned earlier, a large number of ad-hoc networks fall into this category. More often than not, long war driving expeditions turn up a greater percentage of unsecured networks as opposed to secure ones.

Web sites which mention how to participate in war driving are usually not intent on hacking into other networks, but rather to prove that it can be done. "While casual 'war drivers' – individuals who hang around outside companies and look for untended wireless connections – may not get to see your WEP-encrypted data, anyone bent on corporate espionage probably can." Whether the information gathered is intended for the interested wireless user or someone with malicious intent, the effect is the same: vulnerable networks are advertised to the world. These

sites often log the data of other war dialers, making it easy for anyone to easily find vulnerable networks without doing any work. In effect, someone who wants to use an Internet connection without being accountable for their actions needs only to find an appropriate war driving site with a map of their local area marking where vulnerable WAP's are located, then get information from that same site on how to compromise the network's security features.

War dialers who wish to leave tracks for those who follow can learn about something called "war chalking". Similar to a written language often used by hobos to indicate where others might find a hot meal and good place to stay, war chalkers who find an accessible base station can leave their mark nearby with appropriate access information. This information usually includes the SSID of the network, the security status of the network, and signal strength. War chalkers who see the familiar markings are not only saved the trouble of looking for accessible WAP's in a particular spot, but are also informed if a particular network is secured. Not only are vulnerable WAP's frequently logged on web sites for anyone to find, but anyone who knows what the marks mean is instantly informed of an access point without even having to turn their wireless devices on.

Future Solutions

As the number of wireless networks increases, the need for security increases. As discussed, current security features are either ineffective, costly, or non-Universal. Home users want something they can figure out that works without having to purchase anything extra. Network administrators also consider cost, but their primary concern has to be making the network available to most of their users while still offering authentication and protection from intruders.

IEEE's 802.11 Task Group I decided recently to move away from WEP and WEP2. WEP2, with its sliding window implementation and stronger encryption keys, "improves on WEP but doesn't completely address the need for easy, strong encryption." Instead, they agree that additional authentication from a secondary source, such as a RADIUS or Kerberos server, is the direction they want to go. Future versions of WEP will most likely include per-session key negotiation. It is also possible that WEP could develop into something more like SSL, which relies on a certificate authority for key exchange.

At present, several encryption solutions ask users to sacrifice throughput for security. With bandwidth becoming more available to wireless users as 5GHz become widespread, the use of longer keys with longer shared secrets may soon become a solution. While too much throughput is sacrificed for a VPN over 802.11b networks, 5GHz 802.11a networks leave you plenty of bandwidth for VPN security solutions to operate without cutting too deeply into transfers. In addition, over time, VPN clients will become available for more platforms, making WLAN's with VPN landing pads for authentication more accessible.

Many agree that the concept of a security gateway between your base stations and the rest of your network is the best way to go. Future gateway solutions will probably also be based on concepts similar to Archipelago Wireless, where authentication is available without having to download and install a proprietary interface. Wireless users can talk to the base stations but can not get past the security gateway without some kind of acceptable authentication. Future versions of IPSec may be more universal, which would allow a security gateway to maintain a client-free IPSec session between the wireless client and the gateway to protect transmissions.

The second p[art of the paper is to familiarize you with the Bluetooth specification, its capabilities, and associated security concerns.

Technology managers and technicians are constantly engaged in an ongoing struggle between functionality, usability, and security. To effectively balance our concerns, we must keep pace with changes in technology. The telecommunications and computing industries continue to create and market technologies designed to enhance mobility and functionality, both at home and at work. Any organization that desires to exploit opportunities must realize that greater mobility demands a global technology. Bluetooth provides mobility and claims that it will emerge as a scalable, economic global technology.

Bluetooth will become the short-range wireless technology of choice because it provides mobility, security and functionality in one small package. The small form factor of the Bluetooth radio also provides a unique balance of component cost, physical range, bandwidth, and power consumption. The Bluetooth specification is much more than just a cable replacement technology, because it is capable of wireless connections to a wide variety of portable electronic devices via one-to-one, and one-to-many device connections. Bluetooth enabled devices are also capable of simultaneous voice and data connections, as well as, ad hoc networking. All electronic devices that support Bluetooth, or the closely aligned IEEE (The Institute of Electrical and Electronics Engineers, Inc.) 802.15.1 standard for Wireless Personal Area Networks (PAN), will have a 1.5-inch transceiver chip that uses the globally available, unlicensed, Industrial, Scientific, and Medical (ISM) Band ranging from 2.4 GHz to 2.485 GHz (gigahertz). Future development of Bluetooth promises greater functionality and interoperability with other Bluetooth devices, as well as enhanced data transfer capabilities with IEEE 802.11 (Wireless Local Area Networks).

What is Bluetooth?

Bluetooth is an open-source standard that borrows many features from existing wireless standards such as IEEE 802.11, IrDA (Infrared Data Association), DECT (Digital Enhanced Cordless Telecommunications), Motorola's Piano, and TCP/IP to connect portable devices without wires via short-range radio frequencies (RF).

In doing so, Bluetooth inherits the following capabilities:

- Use of the ISM Band
- Frequency-hopping Spread Spectrum (FHSS)
- Authentication
- Privacy
- Power Management
- LAN Capabilities
- Object Exchange Capabilities
- Voice Data Transmission Capabilities
- Ad hoc Networking
- Circuit and Packet Switching

In order to accomplish this, developers purposely chose the free, worldwide available, ISM Band. Bluetooth utilizes an unlicensed portion of the RF spectrum beginning at 2.4GHz, therein providing a globally available communications channel free to all electronic devices, ranging from cellular phones to consumer electronics that support the Bluetooth specification. Bluetooth promises to allow both stationary and mobile electronic devices to communicate, with minimal user interaction, due to its "always on" state.

Bluetooth supports several security features depending on the application, and user requirements. These features range from the protection against eavesdropping, inherent to the frequency-hopping spread-spectrum technology, to the use of keys or Personal Identification Number (PIN), and password combinations. With the use of PINs (alphanumeric strings of up to 16 characters), the 128-bit SAFER+ encryption algorithm is used to create very strong security and encryption between devices. If required, additional security can be added in the application software.

The Bluetooth specification defines three security modes:

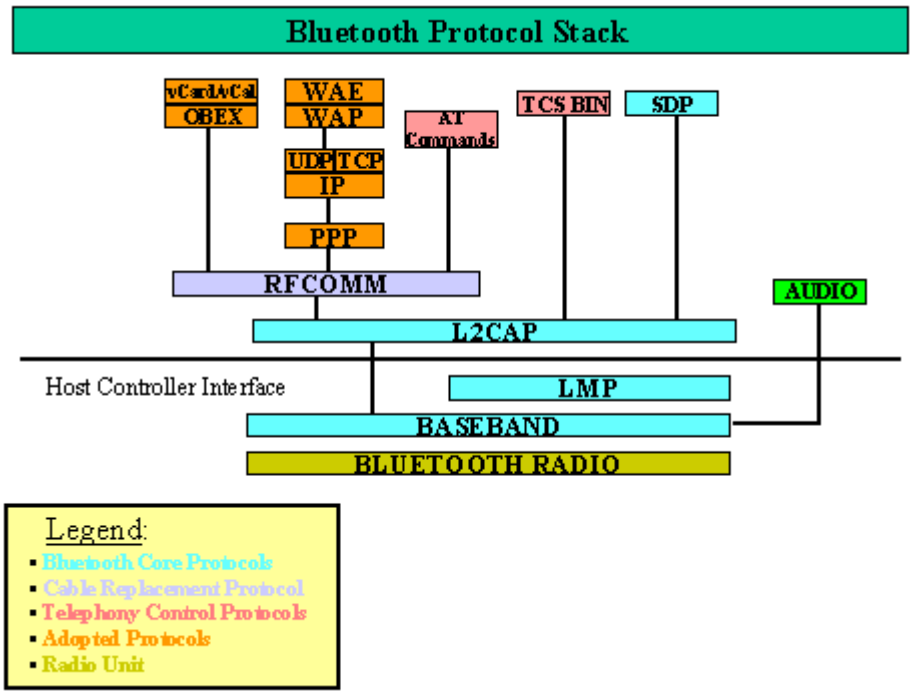
- Non-secure
- Service-level Security
- Link level Security.

In non-secure mode, a Bluetooth device does not initiate any kind of security procedures. It is astonishing that some manufacturers set this mode a default one so that anyone can connect to your PDA and have your full timetable or business information without breaking any law or having to compromise any security system.

In the service-level security mode, security policies are allowed, based upon the access requirements of the application in use. This is especially useful when running several applications that require different security modes.

When using link level security mode, Bluetooth enabled devices set up security procedures before the link set-up is completed. Link level security requires that applications know who is at the other end of the link, in order to, provide authentication, authorization, and encryption services. Information integrity is vital to Bluetooth's future. As a result, developers have incorporated random number generation, encryption, encryption key management, and authentication. Authentication is an important element in any Bluetooth system that enables a user to develop a domain of trusted devices. Once established, authentication services allow the host controller interface to decide if a connection is to be formed based on the available identification at the hardware level. Upon link establishment, additional security may be applied to the data transmission using encryption. Encryption is applied to an existing connection, while authentication procedures dictate whether or not a connection will ever be formed. The security mechanisms inherent into the Bluetooth specification are secure enough for most applications. If not, stronger encryption schemes may be added to Bluetooth products at the software application level.

The security features inherent to Bluetooth are adequate for ad hoc networks, and data transfer of non-sensitive information. Additionally, the 10 cm transmission range of Bluetooth devices operating with a maximum output power of 1 mW provides adequate security for money transfers, and transmission of sensitive data. Information integrity problems will primarily result from users using the wrong maximum output power.



Conclusions

At present, there is no perfect security solution. The only environment that can be confidently secured is one where all machines are nearly identical. For example, a system administrator would have fewer problems implementing an IPSec solution if all computers that wanted to access the network were using an operating system with a compliant IPSec client. A VPN solution becomes acceptable if everyone on the network can be handed a fully-compatible VPN client that works on their pre-arranged operating system. Most security solutions fall short when the solution has to accommodate too many types of possible clients.

Another aspect is the users' understanding of the need for informational security and their understanding of its basics. Your system administrator may be a real talent in security but if you don't follow some simple rules, your corporate information may become an easy prey.

Then there is the issue of cost. Many ad-hoc wireless networks are set up instead of having a wired network to avoid the cost of wiring the building or buildings where the network will be used. The price of purchasing additional hardware and software for security puts many solutions out of reach. The free solutions, which frequently implement WEP, are inadequate and give a false sense of security. If you want to develop a secure wireless network, then you should be ready for costly investments into that security. If not, maybe it is reasonable to wait for the industry to grow and facilitate security by cooperating between huge companies like in Bluetooth SIG.

If the threat of someone reading your traffic or using your network without your permission weren't enough, an increasing number of people out there have made it their goal to discover and expose vulnerable wireless networks. The number of war dialer maps on the Internet increases every day, as does the number of vulnerable networks as the cost of wireless equipment goes down. Whether or not these web sites are designed with the idea of promoting unauthorized activity, someone intent on getting into your network certainly can use the information found on these sites for compromising your network.

As bandwidth limitations and encryption algorithms improve, so will wireless security. It is only a matter of time before someone comes up with a method of providing authenticated access and protected transmission, to the point where wireless security is as the same pace as wired security. Until then, network administrators will have to weigh the pros and cons of every solution available, and hope that they can get their security in place before their network is posted on a war dialing web site as a good place to access the Internet.

References:

1) SANS' Information Security Reading Room http://www.sans.org/rr/
2) Schlesinger, Lee. "The Best Way to Secure Wireless Access." ZDNet: Tech Update. 07 February 2002. http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2845902,00.html
3) Support FAQ, T-Mobile HotSpot. http://www.t-mobile.com/hotspot/support_faq.htm
4) Muller, Thomas. "Bluetooth Security Architecture". Version 1.0. July 15, 1999 http://www.bluetooth.com/developer/whitepaper/whitepaper.asp (February 18, 2001)
5) "Bluetooth: The Official Website" http://www.bluetooth.com/ (April, 2002)