Global Information Assurance Certification Paper

WIRELESS COMMUNICATIONS TECHNOLOGIES: AN ANALYSIS OF SECURITY ISSUES

Jeffrey Posluns, CISA, CISSP, CCNP

GSEC Practical - Version 1.2C

Wireless Technologies

Today's information networks are being exposed to an increasing demand for mobile information. The advent of wireless technologies will introduce many benefits to users of information networks, some of which are:

- Increased efficiency of users' access to information while not at their principal places of operations.
- Ease of use in sharing and transfer of information.
- Increased productivity due to the accessibility of information, regardless of an individual's location.
- Cost-effective network set-up for hard-to-wire locations such as older and solid-wall buildings.

Wireless networks liberate users from their previous dependence on static-location devices to connect them to the network backbone. This freedom to roam offers numerous user benefits for a variety of work environments, such as:

- Location-independent access for network administrators, for easier on-site troubleshooting and support
- Immediate access to patient information for doctors and medical personnel
- Improved efficiency of database access or data entry for roving personnel such as IS auditors, or policy compliance verifications
- Simplified network configuration with minimal IT requirements for temporary configurations such as trade shows or conference rooms

Over the past year, three wireless standards have gained public acceptance and are becoming more widespread in the marketplace: WaveLAN 802.11, Bluetooth, and HomeRF. These technologies introduce new methods of communications and advantages in mobility and ease of use. At the same time, they bring to the wireless world many of the security risks associated with traditional wired networks.

Prior to analysing the risks to information, basic security principals must be established. For the purpose of this paper, we will base the analysis and commentary of security issues on the following principals:

- **Authentication** addresses the issue of identification for the source and recipient of an information transfer.
- **Authorisation** addresses the issue of determining whether the source should be permitted to access the data to be transmitted, and whether the recipient should be permitted to receive this data.
- **Accounting** addresses the issue of the creation of an audit trail for later analysis. This analysis could be to determine usage statistics, for policy compliance issues, or to respond to a security incident.
- **Encryption** addresses the issue of privacy, in that data will not be available to those for whom it is not intended.
- **Control**(s) addresses the use of methods such as the above to enforce compliance or conformity to a policy or standard. This may be a security policy, access control, or other method of enforcing security regulations.
- **Audit** addresses the issue of verifying a device, method, service, or procedure for compliance to policy.

Loss

No specific technology or process directly addresses the issue of loss. As can be seen from publicly available information on security related web sites and mailing lists, there are new software problems and exploits available on an almost daily basis. There is no simple solution to this problem, as there will always be people waiting to find new software vulnerabilities and create attacks and exploits for them. Device and software manufacturers should be responsible for releasing stable products and for maintaining adequate levels of product support and maintenance. Other than software functionality, the ability to release a software patch to a new vulnerability within a reasonable timeframe is what will distinguish the value of one vendor over another from a security perspective. Considering the expected proliferation of wireless communications devices in the near future, and the forced acceptance of them on the market by end users, it is crucial that any security weaknesses found be addressed in an efficient and timely manner.

Malicious misuse by authorised personnel

Once an individual has been authenticated on an information system, there is little in the way of controls that can be done by the device or system owner. The existence of accounting controls (where an independent server or device logs all authentication, authorisations, and access attempts) can allow for the creation of an audit trail. This audit trail can then be queried in the event that an incident is detected, but the process is still roughly analogous to giving your car keys to another individual: there is no way to guarantee that your car will not be stolen. Should the car disappear, then one can form a list of who had a copy of the keys

(verify the logs and audit trail), and potentially determine the individual responsible, but prevention becomes a difficult process.

One significant issue in this regard is the management of authentication systems for wireless devices. In a large organisation with many users exchanging information on their wireless devices, a structured and centrally managed authentication system becomes necessary. Based on current standards, a pair or group of devices must be manually configured for security specifications (keying and/or encryption). As wireless devices such as Bluetooth-enabled personal organisers become more available and are used more strategically throughout organisations, many details will need to be determined:

- Which devices within the organisation are capable of being authenticated
- Which users are authorised to make use of specific services
- What mechanism for establishment of an audit trail exists

The elaboration of these details on a case by case basis will become paramount in the establishment of a secure wireless networking environment.

Unintentional misuse by authorised personnel

As with most technology, the majority of users will not be technologically qualified enough or have the desire to make proper use of their information devices and services. If security is not transparent to the user and application, it is unlikely that the majority of users will make use of it. This is an unfortunate but accepted standard in today's information technology world. From a security perspective, this creates a problem in that one of the following must be done: Device and software manufacturers must make security features simpler and easier to manage, or all wireless devices within an organisation must be configured by a qualified administrator before being given to a user.

This creates another problem because home and non-corporate users are the primary targets for initial sales of Bluetooth devices (according to presentations and discussions at the Canadian Wireless Telecommunications Association conference in Q1 2001). Bluetooth is expected to slowly migrate into the corporate environment, but is not expected to do so for some time. Home users will generally not have the skill sets or desire to make use of security and privacy functions on their devices, and will likely leave them in the default state in which they were sold. In the particular case of Bluetooth devices (and as a general suggestion for the default configurations of other wireless devices) in order to ensure at least a minimally acceptable security configuration, out-of-the-box devices should provide an immediate query to the user with an option for enabling "optimal security settings" and otherwise default to a high level of security. The mechanism for providing this option is up to the individual device manufacturers.

Attack by unauthorised personnel

Monitoring wireless transmissions can be very easy. When one device sends a message over the radio waves, anyone equipped with a suitable transceiver within the transmission's range may be capable of monitoring (sniffing) the transmission. The required transceiver equipment or wireless networking cards are usually very reasonably priced. As the transceiver will perform only passive sniffing, it is almost impossible to determine if someone is intercepting wireless traffic.

Both 802.11b and Bluetooth operate in the w 2.4GHz range using spread spectrum technologies. Spread spectrum was initially developed by the US military to send information that was either hard to detect or hard to jam. While some vendors claim that the devices they manufacture are secure due to the spread spectrum technology that they employ, when the spreading sequence is known to an attacker, there is very little security gained from the technology itself.. Determining the spreading sequence can be difficult, but not impossible.

Data encryption is the only sure method of protecting information in transit. In the case of devices equipped with 802.11 technologies, WEP (Wired Equivalent Privacy) can be used to encrypt data from one device to another. A VPN (Virtual Private Network) with encryption such as IPSec may also be implemented across both wired and wireless portions of the network. This would demand that the wireless-enabled device be able to support the requirements in software (an IPSec stack) and hardware (processing power) for a VPN client. By implementing encryption across the network in this manner, one can reduce – though not eliminate - the necessity for security to be integrated into the wireless hardware.

There are some issues inherent in the use of WEP to secure wireless information transfers. The key used to encrypt data is stored in every user's computer. In the case of a Linux user, the WEP key is stored in clear-text, and can be easily read (in the default configuration) by any user. A user of a mobile device running Linux would generally have at least an above-average skill with computers, and would likely have root access to the system. The user would then be fully capable of discovering the WEP key. In the case of Microsoft Windows, the WEP key is stored in an encrypted form in the Windows registry. Regardless of one's cryptographic skills and tools available, due to the nature of the Windows registry and its use by current wireless device drivers, the encrypted string in the registry can easily be copied to another computer. A simple extract from a first computer, then import to a second will allow the second to make use of the encrypted key, without the user requiring any knowledge of its unencrypted value.

In addition to WEP, some 802.11 access point devices have the ability to restrict access to only those devices that are aware of a specific identification value. Some access point devices also allow for a table of permitted and denied MAC addresses, which would allow a device administrator to specify the exact remote devices that are authorised to make use of the wireless service.

Network administrators are not often given the resources required to maintain security at an acceptable level within their organisations. This is due to the extra time, effort, training, and administration required in implementing security configurations into wireless or wired networks. This would include configuring and maintaining both the encryption built into some wireless networking devices, and the software required for VPN (Virtual Private Network) functionality.

Denial of service

Wireless networks are vulnerable to denial of service (DoS) attacks due to the nature of the wireless transmission medium. If an attacker makes use of a powerful transceiver, enough interference can be generated to prevent wireless devices from communicating with one another. Denial-of-service attack devices do not have to be next to the devices being attacked. However, the attacking device must be within range of the wireless transmissions. The type of equipment required to commit denial of service attacks against wireless networks (making use of today's technology) can be bought for reasonable prices from many common electronic stores. The knowledge required to assemble and activate the equipment can be acquired easily through the Internet or from radio or short wave instruction manuals.

Protecting one's wireless networks from a denial of service attack can be difficult and expensive. A possible solution is to create a faraday cage around the boundaries of the wireless network to be protected. However, this would cut off other wireless communications devices (such as cellular telephones), and would not prevent someone from coming within the cage to activate the denial of service equipment. Thus, while the cage is a possible solution, it may not be feasible. To counter this threat, law enforcement agencies have the technologies to track down wireless denial of service devices in a quick and efficient manner.

Wired networks face the problem of cables becoming stretched, cut, wrongly connected, or otherwise physically abused. Wireless networking devices are a potential solution to these difficulties, as wireless networks are not vulnerable to some of the traditional attacks, such as the denial of service attack executed by simple wire cutters.

The current nature of wireless communications makes it difficult to assure that a signal will be available in all situations and locations, critical or of normal importance. Unless additional assurance beyond standard configurations of devices can be said to prevent denial of service attacks and signal loss issues, current technologies should not be used in situations where consistence of connectivity is an absolute requirement.

Scenarios

Wireless methods of transmission of information within an organisation can offer an attacker access to the internal networks of an organisation that bypasses traditional firewall protections. With wired networks, it is possible to track the location of all wires leading out through core, distributions, and access layers of a

network. With wireless networks, it is almost impossible for a standard network administrator to determine the exact location of all wireless communications devices. Due to the difficulty in determining the presence or location of new wireless communications devices, it is critical that proper authentication mechanisms exist for all parties on a wireless network.

Should an attacker succeed in obtaining a WEP key, a pre-shared secret, or another method of bypassing basic authentication on a wireless network, he/she would then have a starting point for further attempts to compromise nodes within that network. By making use of the acquired WEP key or pre-shared secret, the attacker could make it appear as though a controlled device was an authenticated member of the existing wireless network. The attacker would not need to bypass or compromise a firewall, nor would he/she leave a detailed audit trail. As this type of attack could be performed from outside of the physical structure (office building) housing the wireless network, physical access controls can no longer be considered as effective as in wired-only situations. In order to detect an attacker's attempts to compromise a network, a strict mechanism must be in place to enforce a security policy, as well as performing real-time monitoring to detect illicit activity. Establishment of an audit trail allows for the efficient investigation and analysis of events should any be detected.

A second type of attack in this genre is to make use of a base station in order to make it appear as though the base station belonged to the target network. When a wireless device is turned on, it will attempt to connect to the base station with the strongest signal. Should an attacker have a base station with a high transmission power, the attacker could have the valid network member's devices try to log onto his base station. In doing so, the attacker could potentially acquire what keys or passwords would be used in the attempted logon.

The only protection from these attacks is an efficient authentication mechanism, which would allow the wireless client devices to authenticate with the base station without any disclosure of the secret keys or passwords used to logon to the network.

Conclusion

The current state of security in wireless networking can be divided into two categories. In the case of the home user, security is dependent upon the configurations and options set by device and software manufacturers. In an optimal situation involving a corporate user, security is dependent upon the configurations and options as provided by qualified members of a network or IT department. In a less than optimal situation, it is equivalent to that of the home user.

For wireless communications, ease of use has always been considered a key factor in choosing the device or implementation. As mentioned before, if security is not transparent to the user and application, it is unlikely to be of much use to the majority of the population. The greater the level of security, the more complex the

implementation, administration, and maintenance will be. Network or device administrators will also require a greater level of skill in order to perform their duties.

There is no one wireless technology that is better than the others for all applications; each has its own pros and cons from the perspectives of ease of use, administration, configuration, and connectivity. Each has applications where it is more efficient than others, and the level at which security will be integrated into any device or network will be dependent on manufacturers, implementers, administrators, and the factors that influence their jobs. A security rating can be given to a specific device, service, or application. However, defining a wireless technology as secure or insecure without defining many implementation-specific parameters is not conducive to a proper understanding of the issues previously mentioned in this paper.

In order to assure the security of information stored or transmitted by a wireless device, compliance to an information security policy or associated standards is mandatory. These could be based on a variety of standards, such as the Common Criteria, ISO 13335, BS7799, industry best practices, or other regulations as set forth by a corporation, government, or organisation. Without strict configuration and verification as described above, (taking into account issues such as authentication, authorisation, accounting, encryption, control, and audit) sensitive or personal information may be available to a potential attacker.

References:

Wood, Charles Cresson. Information Security Policies (made easy) Version 7. Baseline Software, 1999.

Schneier, Bruce. Secrets & Lies – Digital Security in a Networked World. New York: John Wiley & Sons Inc, 2000.

Elachi, Joanna. Researchers Find Hole In 802.11 Security. February 06, 2001. http://www.commweb.com/article/COM20010206S0001

Dell Computer Corporation. 802.11 Wireless Security in Business Networks. February 2001. http://www.dell.com/us/en/biz/topics/vectors_2001-wireless_security.htm

Seifired, Kurt. 802.11 Wireless Security. February 07, 2001. http://www.securityportal.com/closet/closet20010207.html

Various. Bluetooth v1.1 Specifications and Bluetooth v1.1 Profiles. http://www.bluetooth.com/developer/specification/Bluetooth_11_Specifications_Book.pdf and http://www.bluetooth.com/developer/specification/Bluetooth_11_Profiles_Book.pdf