Wireless Network Policy Development (Part One)

by Jamil Farshchi
last updated September 18, 2003

The need for wireless policy has never been greater. 802.11/a/b/g wireless networks (WLANs) [1] have taken the Information Technology world by storm. With 35 million units expected to sell in 2003 and with a predicted growth rate of 50-200% compounded year over year through 2006, wireless is here to stay. The benefits of wireless connectivity in the business world are immense; they come in the form of flexibility, convenience, portability, increased productivity, relatively low cost, and ease of implementation. These benefits are not without an expense, though. The same aspects that make wireless so desirable in terms of usability and productivity can also become an Achilles heel if the proper security measures are not addressed throughout the network's life-cycle.

This is the first of a two-part series that helps to create a framework for the most important aspect of a wireless security strategy - policy development. With a solid policy and active enforcement, a WLAN will not only be useable, it will operate with limited risk and most importantly, it will be secure.

802.11 Threats and the Subsequent Need For Policy
The potential threats to WLANs are numerous. Denial of Service (DoS), session hijacking, and sniffing are just a small sample of the potential attacks. While many of the attacks against wireless networks are similar to those against wired networks, 802.11 networks are generally subject to more threats.

One of the more serious problems is Wired Equivalent Privacy (WEP), the data encryption standard for wireless networks. WEP has been found to have weaknesses [2] and can be "cracked" in as little as a couple of hours.
Another problem is related to the open nature of WLANs. Due to the propagation characteristics of wireless networks, there is limited control of where a signal is accessible. This leads to a situation where, unlike wired networks, a hacker can manipulate or eavesdrop on the network from uncontrolled locations or geographical areas which were not intended to be served when the network was implemented.

WLANs can also create backdoors to wired networks. Many organizations spend thousands or millions of dollars on wired network security with extensive investments in firewalls, VPNs, and other security-enhancing technologies. A single unauthorized (rogue) wireless access point (WAP) connected to a wired network has the potential to create a backdoor to the wired network, circumventing the wired network security and thereby allowing a hacker to effortlessly gain access to a closed network. A wireless policy can help combat these threats. Fortunately, it is never too late to develop a policy, although an early adoption approach is highly effective.

Early Adoption
Policy development should begin in the conceptual stages of a wireless network initiative. The benefits of realizing and addressing the need for security at an early stage in the development process are immense: lower cost, easier implementation, and security from the onset of implementation. To add security after an implementation, new equipment may need to be purchased, the network may need to be logically or physically redesigned or worse -- the network may have been exploited during the period of weak security. If the network has been in operation without security, a policy will still provide numerous benefits, although the benefits will come at a higher cost than if the network had been implemented with security from the onset.

Benefits of a Wireless Policy
A wireless policy will not eliminate the threats to 802.11 networks. But it will help create a proactive environment where the tools, methods, and procedures are in place to deter attackers and combat the threats effectively. A policy establishes a security model for the existing or the

soon-to-be-developed network. A good policy creates a set of rules and standards for users, administrators, and managers to follow. The policy can bolster awareness of security and proper usage techniques. It will guide all future wireless implementations, ensuring that expansion efforts are uniform and compatible with existing 802.11 implementation(s). Policy allows network manageability, appoints enforcement authority, and facilitates accountability.

The Essential Components of a Wireless Policy
A security-conscious mindset is the cornerstone to any successful wireless policy. By viewing security as an integral part of the network, a manager can properly integrate security with functionality from the onset. A proactive security approach will greatly improve the security posture of the entire network.

Wireless policy can provide guidance on a wide variety of issues specific to the organization, but there are several issues that should be considered with most wireless network policies:

Note: The following list of policy considerations can be used for both open [3] and closed [4] wireless networks, although some of these considerations will not be applicable to an open wireless network.

Delegation of Authority and Responsibility
The policy should appoint an authority figure who has responsibility and authority of the wireless network. Appointing an authority figure will provide direction, leadership, and accountability for the wireless network(s) through development, implementation and ultimately, operation. This "security manager" will be in charge of all network security functions and will have the authority to appoint other individuals and/or create teams if necessary. This person will also have the ultimate responsibility of ensuring the proper security measures for the network have been deployed, and subsequently, will be the official with the utmost accountability.

It is important to delegate the authority of the wireless network to someone who is also responsible for the network. If the individual is not given a stake in operation of the wireless network, the individual will be less likely to take the measures necessary to ensure the proper functioning of the network. It is also beneficial if the individual appointed is someone who has experience and understands the issues inherent with a wireless network.

Risk Assessment
The policy should require a risk assessment. A risk assessment will determine the threats and vulnerabilities of the organization in relation to WLAN operation. Understanding risks will help protect against unforeseen threats, delays, and costs, as well as allow an adequate number of security features to be implemented. The security manager (the individual who has been delegated authority and responsibility for the wireless network) should employ security measures in conjunction with the risks associated with the 802.11 network. For example, if the network is only used for casual web surfing, the risk of loss in the event of an attack may be minimal. If, though, the network is used for transmission of business sensitive material, classified communications, or supports critical services, the risk of loss in the event of an attack or loss of service may be extensive. A risk assessment needs to be conducted to ensure the scope of the security measures will be adequate for the risks associated with the network. A risk assessment can be scoped to identify data sensitivity, network vulnerabilities, critical services, and personnel deficiencies, among many others. The focus should be to identify potential threats and vulnerabilities in the event that a wireless network is implemented. In some cases, the threats to a wireless network may outweigh the benefits of the technology, in which case the network should not be allowed.

In the event that a WLAN is implemented, the security policy should be developed in concert with the total risk to the network.

Threats and vulnerabilities are ever-changing so risk assessments should be conducted on a regular basis to provide an accurate picture of the total risk to the organization. The policy should therefore define the frequency of risk assessments.

Network Segregation
Policy should require separate and distinct wireless and wired networks so that a security breach on a wireless segment will not as easily affect the wired network(s). Network segregation provides a way to separate the "untrusted" WLAN(s) from the more "trusted" (and usually wired) portions. WLANs usually connect to a wired network at some point to facilitate Internet or Intranet communications, and the convergence of these networks should be separated by a gateway so that wireless communications are not required to traverse the wired network unless necessary. In addition, a filtering device (like a firewall) can be placed between the wired and wireless networks to control and monitor the traffic between the wired and wireless segments. The device will aid in the separation of the networks as well as provide a layer of protection for the networks.

Figure 1: Example of a segregated wireless network
Authentication
Authentication is essential to the secure operation of an 802.11 network and should be included in the wireless policy. All users of WLANs should be required to authenticate before being allowed to access the network. Authentication provides a means to limit access to a closed resource. There are a number of issues the wireless policy should address in relation to authentication.

Policy should address the authentication standard, method, implementation, and maintenance requirements. First and foremost, policy for wireless network authentication should follow the latest standard. It is highly advisable to follow the standards when selecting an authentication solution (more explanation of the standard in the next section). Conforming to standards is beneficial because it alleviates the risk of implementing a proprietary technology and subsequently committing to a specific vendor.

Secondly, a form of mutual authentication should be defined in the policy (the authentication standard may define this already). With mutual authentication, both the client and the server are authenticated to each other. Mutual authentication primarily adds security by establishing the authenticity of the server, but this method of authentication also enhances security in other ways, such as reducing the ease of rogue network proliferation. Another factor to consider with authentication policy should be ease of implementation and administration. Some forms of authentication, such as Public Key Infrastructure (PKI) [5] solutions, may be secure, but incur extensive implementation and administration overhead.
The policy can also indicate the strength of the authentication, as well as provide guidance as to whom, when and for what resources authentication is required. The policy may define the user and group access levels, how access will be managed, and any necessary implementation specifics.

Confidentiality
A means to assure confidential wireless communications should be defined in the policy. Encryption can provide a secure communication channel for which wireless transmissions can occur without the threat of eavesdropping. Without encryption, it is trivial for a hacker to gather sensitive information transmitted to and from a wireless network. Wireless network signals offer hackers the ability to stealthily gather wireless data in an anonymous manner. A number of issues should be considered when including confidentiality into the policy.

Policy should define a reasonable encryption method so that wireless communications can be transmitted with confidentiality. The basic encryption method employed with 802.11 communications is Wired Equivalent Privacy (WEP). Unfortunately, the WEP algorithm can be decrypted and rendered useless. Nevertheless, WEP offers some protection and should therefore be defined in the policy if no other encryption is possible. To combat the insecurities of WEP, other encryption options are currently available and should be used instead, if possible.

The IEEE 802.11i standards group is currently developing the standard for 802.11 security. The standard is expected to standardize the use of Temporal Key Integrity Protocol (TKIP) as an alternative to WEP. Furthermore, the 802.11i standard will offer Advanced Encryption Standard (AES) as the encryption algorithm of choice. However, at the time of this writing 802.11i is not yet published and security will be needed on the wireless network in the midterm. The WiFi Protected Access (WPA) is a subset of the IEEE 802.11i draft standard and is designed to be forward-compatible with 802.11i when it is finally published. WPA should be followed because conformance to this standard will allow a (hopefully) relatively seamless transition when 802.11i is published. If following WPA or 802.11i is not an option, there are also many other solutions including a Virtual Private Network (VPN). Even the use of the weak WEP encryption will help improve security -- although modestly. While the lack of published standards is deterring, encryption must be included in the policy.
The policy should address the encryption strength, method, implementation, maintenance (such as key rotation), and frequency of use. The strength of the encryption should be chosen based on the sensitivity of data that will be traversing the network -- the more sensitive the data, the higher the encryption factor. The method defines the encryption to be used and the implementation should describe how the encryption will be deployed. The frequency of use should define when the encryption must be used. For example, if a user is dealing with sensitive data, encryption should be mandatory; other situations should be evaluated accordingly.

Availability
To ensure maximum network uptime, wireless availability tests should be defined in the policy both in terms of operation and frequency of execution. Availability of WLANs is essential because productivity is a function of downtime. Wireless availability tests should be conducted before deployment and during 802.11 network operation to ensure adequate signal coverage and an environment that is free of conflicting RF transmissions.

802.11 networks are fraught with Radio Frequency (RF) conflicts and impeders. If availability tests are not defined in the policy and executed in a timely manner, the network may suffer from poor signals in the long-term. One of the problems is that many natural and physical objects cause RF signal degradation, such as trees, rain, earth, buildings, etc. To add to the transmission issues, common devices such as cordless phones, baby monitors, Bluetooth, and microwave ovens transmit on the same frequency as 802.11b/g networks. 802.11a networks operate on currently less trafficked bands, but are still susceptible to interference from newer cordless phones, etc. RF conflicts and/or spotty signal coverage can cause wireless networks to be denied service.

Many tools exist to aid in wireless availability tests. Topology software can be used to identify any naturally occurring obstructions such as hills, valleys, etc which would potentially limit transmissions. Topology tools can work well to identify potential issues before wireless deployment. If topology tools are used, they should be specifically referenced in the policy.

Figure 2: Example of the results of a wireless availability test. This image depicts a wireless signal propagating beyond the building it is indented to serve and onto public streets.

Wireless availability tools will identify locations with weak 802.11 signal strength. 802.11 client software (such as the Cisco Aironet Client Adapter software), can be used to adequately assess signal strength throughout a wireless coverage area. A relatively simple method to conduct availability tests is to walk or drive throughout a wireless coverage area with wireless client software, while noting areas of weak signal strength. Like topology tools, the availability testing tools should be specifically defined in the policy.

The policy should force the execution of wireless availability tests, indicate the specific testing tools, provide a reasonable frequency for which the tests are to be conducted, and define a time-frame for test completion. While wireless networks will undoubtedly encounter interference from

time to time, defining availability tests and tools in the policy and the subsequent execution of these tests will help reduce signal loss and improve availability.

NOTE: Due to the wide array of devices operating at the same frequencies and the subsequent ease of denying service, wireless networks should not be used for mission critical applications or services unless absolutely necessary.

Concluding Part One
The upcoming second and final article in this series will continue the discussion of essential components in a wireless policy, including logging, WAP physical security, client-based security, wireless scanning, education and awareness, and other considerations. Together, these two articles on 802.11 wireless policy development will help create a WLAN framework -- one that is not only useable but operates with limited risk and in the most secure manner possible.

References
[1] 802.11a/b/g is the set of Institute of Electronics and Electrical Engineers' standards for wireless computer communications.
[2] Berkeley WEP Security Analysis Presentation
[3] An open wireless network is one that allows all clients access to the network resources.
[4] A closed wireless network is one that only allows access by authorized users.
[5] PKI

Wireless Network Policy Development (Part Two)
by Jamil Farshchi
last updated October 2, 2003

Part One of this article explained the need for wireless policy, some of the inherent threats of wireless networks, and covered some of the essential components of a wireless policy. This second and final article will continue to discuss essential components for policy development, as well as address other considerations that one should be aware of. Taken together, this series of articles on wireless policy development will help create a framework for an organization's wireless policy, its active enforcement, and will allow a wireless network to be both secure and operate with limited risk.

The Essential Components of a Wireless Policy (continued)
Logging and Accounting
Logging and accounting serve a variety of beneficial purposes and should be mentioned in the policy. Logging and accounting aid in activity tracking, accountability of use, and misuse detection.

The policy can include accounting, which is best used to monitor and/or track user usage and can be satisfied with a service like RADIUS.
Logging is essential and should be an addition in the policy for several reasons including user monitoring, debugging, and accountability. Logs can help identify and track an intruder in the event of a security incident, aid in the debugging of a problem, and provide a source for a variety of information. Logging can be accomplished with a WAP, a firewall which separates the wired and wireless networks, with backend authentication servers, and/or on the wireless clients. A wireless web logon interface (if used) can also provide a means for logging activity.

Policy should also define the frequency that logs are to be reviewed. Logs should be reviewed and maintained on a regular basis to provide maximum effectiveness.

Wireless Access Point (WAP) Security
Wireless policy should explain the need to both logically and physically secure WAPs. Access points should be located in physically secured areas. These devices should also be setup to only allow administrators to make configuration changes. Most WAPs, when reset, will revert to a default (insecure) mode. If the WAP is in an unsecured or heavily trafficked area, it is easy for someone to physically manipulate the access point and turn it off to deny service or reset it so that it reverts to the default configuration. The WAPs should also be adequately secured so that unauthorized individuals cannot connect to and manipulate the secure configuration settings. Most WAPs allow the creation of accounts and passwords for authorized users. These accounts should be created to limit unauthorized access to the WAP.

The policy should describe which users are allowed to connect and administer the access point as well as define what systems the administrators are allowed to connect to the WAPs from. Policy should also require that the WAPs are located in a physically secure location.

Client-based Security
Wireless policy should dictate the security measures employed on the wireless clients. Wireless clients are typically numerous and operated by users with a varying degree of technical affluence. This lack of technical prowess can lead to a complete lack of security on the user-controlled wireless devices.

Wireless clients should be equipped with (at least) a host-based firewall and anti-virus software. Often a weak link in the security chain, wireless clients can become targets for attack and then once compromised, used as a launch point for subsequent attacks. Wireless clients are naturally more difficult to secure due to their mobility and subsequent dependence on the user to apply proper security measures during use. Hackers can use many attacks directed at wireless clients so it is essential to implement some host-based security on the user-controlled wireless devices. Wireless policy can and should define the use of firewalls and anti-virus software. Policy should also disallow the use of ad-hoc wireless communications.

Firewall. The policy should require the use of a firewall. A host-based firewall will limit the wireless client's exposure to threats. A firewall will help to mitigate the wireless client's risk by denying any network traffic that fails to meet the security policy. A firewall is also an excellent method of logging wireless activity.

Anti-Virus. Policy should address the use of anti-virus software as well as the frequency of mandatory definition updates. Anti-Virus software will help protect the wireless client from a variety of threats. Not only can viruses destroy critical data on the client, there are viruses that, when executed, will create backdoors on the client. If a client system is compromised by a virus an attacker may have the privileges of a legitimate wireless user and can therefore attack other wireless clients, or even utilize trust relationships to attack the wired network. Anti-virus software will attack the virus threat upon detection and will subsequently minimize the risk of a client system compromise. While anti-virus software enhances the security of the wireless client, without updated virus definitions, the software can be rendered useless. Therefore, policy should specify both the anti-virus software as well as the frequency of mandatory virus definition updates.

Ad-Hoc communications. Policy should disallow wireless clients to engage in ad-hoc communications. These ad hoc wireless networks allow two or more stations to communicate directly with each other without an access point routing their traffic.

Hackers can conduct a number of attacks against systems using ad-hoc wireless networking. The primary issue with ad-hoc networks is the lack of authentication. Ad-hoc networks can allow a hacker to execute man in the middle attacks, denial of service, and/or compromise systems.

If a hacker can compromise one wireless client, the attacker can use the system to attack other systems on the network. If the wireless clients cannot communicate with each other initially

(through an ad-hoc configuration), it is more difficult for a hacker to attack or gather information from the network.

Wireless Scanning
Policy should define the execution of wireless scanning, identify the tools to use, and define the frequency of scanning. Scanning provides a method to locate rogue (unauthorized) access points. This activity is referenced by many names, including wardriving, warwalking, warbiking, etc, all based on the method of locomotion used to conduct the activity. There are also some scanning solutions that allow strategically placed nodes to continually scan for wireless networks.

Figure 1 -- Example results of a common scanning tool.
This image shows both encrypted (red) and unencrypted (green) networks for the given scanning location.

Rogue access points can be installed by individuals (internal or external to the organization) and present a substantial security threat. These access points can create backdoors, inviting hackers to exploit the network. Many times, these rogue access points are installed with good intentions (a power user wants roaming access to increase productivity for instance), but they can also be initiated by hackers looking to exploit wireless users. The introduction of these rogue access points poses an immense potential threat to the network. Policy should provide guidance to scan for and eliminate rouge access points.

Scans should be conducted on at least a weekly or monthly basis to be optimally effective. Policy should define the execution of wireless scans, identify the tools to use, and require that the scans are conducted on a regular basis.

Education and Awareness
The policy should include provisions for increasing and maintaining security awareness of all users. Arming users, administrators, and managers with wireless security knowledge and awareness enhances the security posture of the entire network. Teaching individuals about wireless threats creates a security conscious environment. If the wireless network users, administrators and managers are aware of the security issues, they will be more apt to take the steps necessary to secure or at least limit, the activities that put the network at risk. Furthermore, if the administrators and managers are taught how to secure their systems and informed of the latest threats to the wireless technology, the benefits are two fold. Not only will the individuals realize the security issues and take steps to limit the risk (for example, do not use sensitive login/passwords on unencrypted wireless sessions), they will be armed with the knowledge allowing them to actually secure their systems (example: enable encryption, etc..). The best example of this is the adage, "Give a man a fish and he will eat for a day. Teach a man to fish and he will eat for a lifetime." By proactively offering information on wireless security to users, administrators, and managers, the individuals will likely take a more prominent role in securing the network.

Policy should allow for the education of users and define specific measures to increase awareness of wireless network security.
Others Considerations
The wireless policy can also address other issues that may or may not offer additional security depending on the wireless implementation, architecture, and other security methods employed for the network.

Static ARP Addressing
Policy to require static ARP addressing can enhance security, but at a great cost to administration time. By statically assigning Address Resolution Protocol (ARP) addresses, the network will be protected against spoofed ARP attacks. ARP can be manipulated by spoofing to reroute network traffic to a malicious host. Static ARP addressing will not allow a hacker to spoof ARP replies. Statically assigning ARP addresses can be a difficult and time consuming task for administrators on a highly populated network.

MAC Filtering
Wireless policy to force the use of MAC filtering should be employed only if administrative time is not a concern. Media Access Control (MAC) filtering on the access point provides an added layer of authentication for wireless clients. MAC filtering will only allow authorized MAC address to connect to the access point. This technique is time consuming to maintain on a highly populated network. Also, MAC addresses can be spoofed, therefore allowing hackers to imitate legitimate MAC addresses and circumvent this security measure.

Static IP Addressing
Like MAC filtering, the addition of the measure into the policy should only be employed if administrative time is not a concern. Static Internet Protocol (IP) addressing forces wireless clients to have a legitimate IP address before access to the network is granted. Dynamic Host Configuration Protocol (DHCP) is the alternative method for address allocation, where clients simply request an address from the DHCP server and the server allocates an address for them dynamically. Static IP addressing forces hackers to know the network addressing scheme and manually allocate an address. It is still possible for hackers to find legitimate addresses, so this measure adds minimal security.

SSID Naming
Policy should define an SSID naming scheme and require all wireless networks to be identified accordingly. The Service Set Identifier (SSID) is simply a wireless network identifier that can act as a password when a mobile device tries to connect to the WLAN and broadcasting the SSID has been turned off. The SSID should be named something that is not intuitively linked to a project, organization, or individual that the network serves. SSIDs provide hackers a method to easily focus attack efforts on a specific network. For example, if a hacker wanted to attack the accounting program of an organization and the office's SSID is named 'Accounting_Dept', it would be trivial for a hacker to focus efforts on that specific network.

SSID Broadcasting
Wireless policy can disallow the use of SSID broadcasting to make access points more difficult to identify. Traditionally, access points broadcast their presence for anyone with a wireless client to hear. In many cases, this feature may be turned off because it causes the wireless network to announce its presence, potentially to hackers.

There are tools that can identify access points even if broadcasting is turned off, but this still may be a beneficial option to disable.

Wireless Intrusion Detection
Consider including policy for a wireless intrusion detection system (IDS). A wireless IDS can improve security in a number of ways including, detecting wireless activity/attacks and aiding with policy enforcement. There are some unique challenges to implementing a wireless IDS due to the propagation characteristics of wireless signals and the potentially expansive geographical footprint a WLAN can encompass. There are currently both commercial and open source wireless IDS solutions which will monitor 802.11 transmissions.

Policy to include the use of wireless intrusion detection systems should address deployment/implementation as well as define the IDS device (or software). Policy should also require the review of alert logs at a regular interval.

Enforcement
Once the policy is completed and distributed, it must be enforced! Without enforcement, there is little benefit to developing a policy. Everyone in the organization should be aware of the policy and it must be followed. Current and future network operations and development should follow the policy as well. Enforcement of the policy is absolutely essential for the network to be used, and to perform as planned.
Conclusion

Wireless networks provide users with an immense amount of freedom. Pushed by many high technology companies as the next "big thing," wireless is not only easy to use it is also being heavily promoted. Unfortunately, little is mentioned of the broad array of security deficiencies wireless technology is laden with. To make matters worse, in an effort to make installation easy, almost all wireless hardware/software vendors ship their products configured with insecure settings by default. Therefore, wireless tends to be easy to install, but relatively difficult to secure. These issues make the presence of a wireless policy even more pertinent.

Fortunately, there are steps that can be taken to help address the security issues with 802.11 technologies. Each network will inherently have its own specific configuration needs, but by having security conscious mindset and following a few policy guidelines, a wireless network can be secure. By implementing a sound security policy and following with thorough enforcement of that policy, an organization will be well equipped to face the security challenges that wireless technology presents. With these steps in place, a wireless network can provide the added functionality of a cordless environment with the improved security of a hard-wired solution

References
Wireless Network Policy Development (Part One)