

## Wireless Policy Development (Part Two)

*Jamil Farshchi* 2003-10-02

**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.

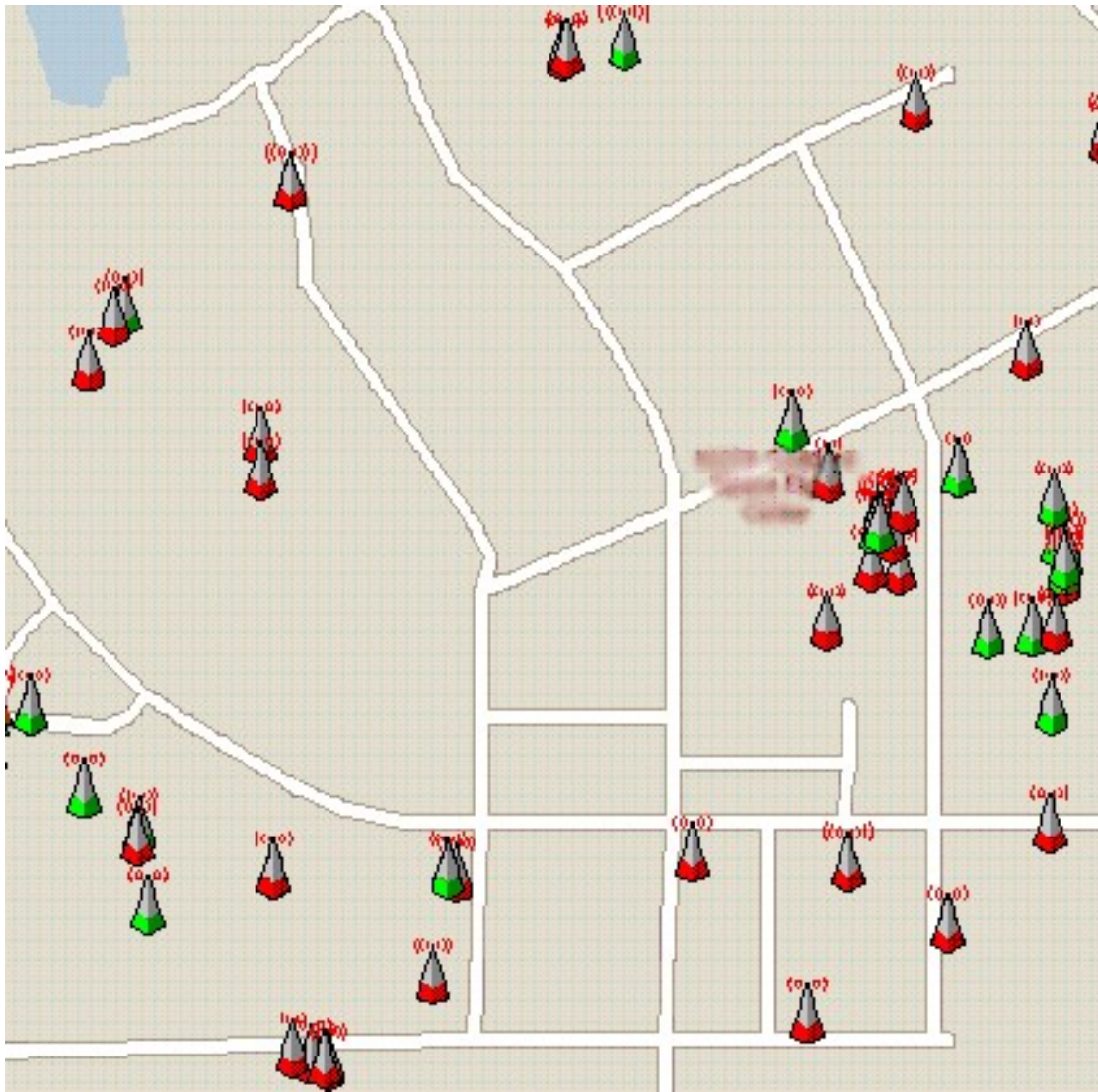
**Ad-Hoc communications.** Policy should disallow wireless clients to engage in ad-hoc communications. These ad hoc wireless networks allow two or more stations to communicate directly with each other without an access point routing their traffic.

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 rogue 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 \(Part One\)](#)

[Privacy Statement](#)

Copyright 2006, SecurityFocus