Global Information Assurance Certification Paper

Wireless IDS: Exposures, Attack Vectors, and Detection

Birchard P Hayes

Abstract

Wireless networks are quickly becoming a feature in many people's lives and offices. Corporations are exploring new collaborative paradigms that leverage the flexibility of Wireless LANs, Executives are using public Hotspots to stay connected while out of the office, and consumers are extending their broadband home connection without having to lay down an CAT5 cabling. Vulnerabilities and exploits have also become a feature of the adoption of Wireless Networking, frequently outpacing the technological ability to mitigate those weaknesses. Wireless Networking is here to stay and it is not inherently secure. The network security professional must use all of the tools at their disposal to maintain the confidentiality and integrity of the assets entrusted to their networks. Wireless functionality has also become so common that any security plan must consider 802.11 network vulnerabilities and the 2.4GHz spectrum even if there is no intention of deploying Wireless Networking.

Wireless IDS is becoming a larger part of the security professional's toolkit. Early and accurate detection of network misuse or compromise is the last bastion of defense in an environment where client nodes cannot be hidden behind a firewall. The old maxim of "physical access always wins" has been superseded when the network medium itself cannot be limited physically. Where it previously required sophisticated gear to eavesdrop from outside a building, Wi-fi now gives anyone with a wireless client adapter and a few readily available software tools that same functionality. The exposure of the network increases with the determination of the attacker and the time the attacker is allowed on target. There are commercial systems and services available to those with corporate sized funding and there are good Open Source tools available to the technical minded. However, there are still no tools for the typical consumer, who remains unprotected as has been the case with other IP technologies. The available solutions are not in themselves sufficient and must be deployed as part of a strong overall security plan. There still remain lessons to be learned from the early history of cell phones and necessary improvements to the existing offerings of Wireless IDS tools; however the current offerings go a long way to dissuade the casual or amateur interloper.

Introduction

As Wireless Networks have become more commonplace in both office and home environments it has become increasingly clear that a new security paradigm is required to provide the same level of security afforded traditional, fixed wire networks. In the wireless world there is no longer the physical security of cable runs within a controlled and protected building. DSL has removed the ability to limit corporate users connecting from home by using 'dial back' modem connections and Wi-fi increases the exposure along this attack vector, as it is becoming the home networking medium of choice. The key to securing this new paradigm are Intrusion Detection Systems; traditional IDS to continue to protect the corporate LAN behind the firewall and, now, Wireless IDS to protect the airwaves in and around the corporate LAN.

To use the metaphor of physical security, locks and gates only serve to slow down intruders, while active defenses are useless without strong detection abilities. Nothing keeps the wolves at bay quite like a loud, barking watchdog whose alarm causes dark corners to become bathed in bright light. In the same way, no network, particularly a wireless network, can be secured without active monitoring that allows the actions of an intruder to be quickly revealed. Unfortunately, a network compromise due to 802.11 Wireless Networking could occur regardless of an organization's network usage and security policies. So many computers come equipped with Wi-fi embedded, enabled, and roaming, that even a well-meaning end-user can unintentionally open the network to attack. Any organization seeking to secure its network must at least deploy Radio Frequency monitoring, while an organization that intends to utilize Wireless Networking in its operations would be strongly advised to deploy a multi-layered Intrusion Detection System.

The Playing Field

The deployment of Wireless Networks runs the gamut from intentionally open, public systems to unintentionally open, private residential systems to closed, secure government systems, although some are less secure than others.[i] Businesses seem to fall across the entire range; some implementing best-in-class security and others unintentionally leaving their corporate network and other assets open for the public to access. Home users are particularly vulnerable, as is frequently the case, due to lack of expertise and dedicated LAN staff to configure their computers and connections. Corporate users working from home can inadvertently compromise an organization by using Wi-fi to connect to a DSL or cable modem. While some individuals and organizations have intentionally opened their bandwidth to their communities and the public at large, many networks have been naively left open. Manufacturers have generally chosen ease of installation over consumer protection, so almost all 802.11 Access Points will accept connections from anyone and Wi-fi network client adapters will associate with 'any' WLAN.

There are many good books and white papers, a few of which are listed in the Suggested Reading section that address the basics of 802.11 Security, thus those topics won't be reiterated in this paper. However, both the proliferation of Wireless Networks and articles defining WLAN security short comings, in addition to so many computing devices being supplied with Wi-fi installed and enabled, are continuously increasing the likelihood that an organization will have a problem involving Wireless Networking. Currently, the best practices for deploying a WLAN are certificate-based VPN or a WPA encrypted, managed connection to a hardened, closed-network Access Point. Ad hoc, or peer-based, networks should be avoided, as should the inherently weak WEP encryption. Corporate policies must detail remote connections into the corporate LAN and plans to support home-user Access Points should be crafted if VPN clients cannot be deployed. An effective Security Plan should include firewalls and a multi-layered Intrusion Detection System.

War-driving, biking, boating, and other variants have reached a wider audience and are now the domain of hobbyists, script kiddies, and network administrators, in addition to the community of skilled adversaries, a.k.a. 'Black-Hat Hackers' or Crackers. Currently,

War-driving is not unlawful, in contrast to its predecessor, War-dialing, which is a prosecutable offense.[ii] Many hobbyists maintain that the geographical mapping of Wireless Access Points is a benign past time and that it is only the circumvention of security measures to obtain a network connection that is 'hacking.' Even well intentioned journalists are guilty of 'borrowing' bandwidth[iii], although law enforcement officers are apparently beginning to consider 'theft of signal' to be serious enough to challenge citizens engaging in outdoor Wireless Networking.[iv] Even if War-driving becomes unlawful, it is entirely too simple to limit the transmitting capability of wireless gear and eavesdrop without being detected. Wireless Sniffers, WEP Crackers, and other 'script kiddie' tools are far too available to underestimate the level of risk posed by unmonitored airspace, unapproved Wi-fi devices, and users connecting across 802.11 home networks into the corporate LAN. A Google search for War-driving or, its companion activity, War-chalking (the marking of discovered WLANs) will yield hours of hypertext reading.

While it is unlikely to ever become cost effective to deploy Wireless IDS sensors at every employee's residence, it is entirely foolhardy not to deploy some kind of RF Monitoring at an organization's location regardless of whether or not Wi-fi is allowed in the security policy. If WLANs are a part of an organization's network plan, then great care should be taken to secure all connections and communications, and even greater care should be taken to monitor the radio frequency airspace around the WLAN. Current Wireless IDS offerings are not yet sufficient to provide a resilient, in-depth defense by themselves; however, this reflects the factor of development time and building market demand rather than critical shortcomings. Traditional, wired LAN Intrusion Detection should still be deployed to monitor and benchmark all network traffic in order to minimize the impact of what ought to be considered an inevitable network penetration.

Attack Vectors, Signatures, and Detection

The currently identified potential attack vectors are Poorly Configured Access Points, Rogue Access Points, Bogus Access Points, Wireless Clients, and Denial of Service attacks. Some of these attack vectors can be mitigated by good system administration, particularly configuring Access Points, while some cannot be mitigated at all. Denial of Service against a WLAN only requires the generation of sufficient Radio Frequency noise. There are also Wide Area Wireless LANs and Personal LANS to consider; Wide Area network end points could be covered by Wireless IDS, except for the prevention of eavesdropping, while Personal networks create new issues.

Many of the scripted attacks have detectable signatures. Netstumbler for instance has a very specific behavior, probing a discovered Access Point for SMB information, adding unique ASCII strings into the payload, and similar identifiable traits.[v] Several Commercial IDS systems utilize pattern matching to detect known attacks. However several attack vectors are passive in nature and eavesdropping can always be performed without revealing the attacker's presence. WEP cracking tools can be run against recorded traffic gained during an eavesdropping session, which might allow an attacker to return with a subtle approach thus gaining access without using common, 'script kiddie' tools. An effective Wireless IDS must include both pattern matching, to stop

easily identified exploits, and a heuristic or behavior matching ability, to discover malicious behavior within normal traffic.

Personal Local Area Networks [PLANs], generally using Bluetooth or Infrared to communicate between devices, are also a vulnerable attack vector, although due to their intentionally limited transmission strength they have not received the attention of 802.11 based networks. Bluetooth PLANs are most vulnerable in crowded, public spaces, like train stations, than in a typical office environment where the risk centers on the insider threat. The exploits are harder to find but the basics of Bluejacking are becoming easier to find on the Internet[vi]. There may possibly be a time when Bluetooth Intrusion Detection or Firewalls will be necessary to protect information stored on Bluetooth enabled devices, however the threat has only recently been identified so mature tools have not yet been developed; although Full Mesh Networks has included Bluetooth discovery to their service offering[vii].

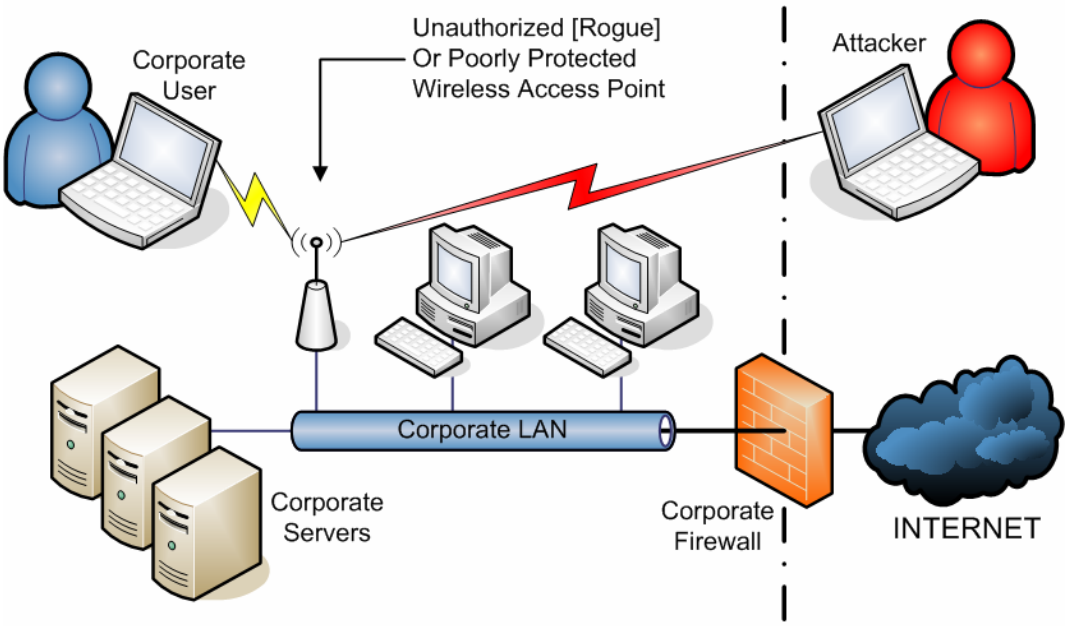

Figure 1

The Poorly Configured Access Point is an approved Access Point that has been left in its default configuration or some defaults remain. System Administrators may turn on WEP encryption and MAC address filtering, but allow administration over the Wireless side of the Access Point rather than limiting administration to select IP Addresses from the Ethernet side of the AP. WEP can be broken, MAC addresses can be faked, and the default Administrator passwords for all Access Points have been published; leaving the configuration interfaces open to wireless clients allows the intruder full run over the AP in addition to network access. [Figure 1] Connecting to a network through an open, unprotected Access Point really should not count as an attack vector because it is trivial by design. Access Points will, generally by default, accept and route connections from any wireless client. While WPA encryption and the upcoming 802.11i standard will raise the bar, it appears that only certificate based authentication can reliably close the door,

bypassing the vulnerability at the Access Point by creating an authenticated, encrypted connection into the network. Cranite's WirelessWall server is a good example of Intrusion Prevention rather than Intrusion Detection using this principle.[viii] It uses certificate based authentication and encryption to limit connections at the Access Point in addition to protecting the transmission from eavesdropping by creating an encrypted tunnel.

The Rogue Access Point is typically the result of an individual, or department within an organization, deploying Wi-fi equipment without authorization or administration. Enthusiasm for new technology or a deliberate circumvention of existing LAN policies can lead to unprotected or poorly configured Access Points being introduced onto the organization's LAN. This phenomenon is similar to the proliferation of 56k modems that made War-dialing an organization's range of phone numbers part of any good security audit. As faster modems became cheaper and easier to install, it seemed that the more restrictive an organization's Internet use or security policy was, the more likely it was to discover unauthorized modems in user machines during an audit. The Rogue AP presents the same vulnerability as an unapproved modem; connections can be bridged from the wireless to Ethernet essentially creating a back door into the organization's network. Unapproved and undiscovered Access Points and Ad hoc networks can only be reliably detected by monitoring radio frequencies; policies and audits may eliminate most but not all unauthorized devices.

Similar to the Rogue Access Point is the Peer-based, or Ad hoc, network in which two or more client computers form a network based on file and printer sharing. The Ad hoc network presents a greater threat because it is, by definition, unmanaged and thus easier to hijack. Furthermore, Ad hoc networks do not require any additional hardware; any two wireless client adapters can create a 'workgroup' type network that would not necessarily be visible on the wired LAN. Ad-Hoc networks do have their uses however; peer or cooperative networking can create a flexible, deployable network for Emergency service and response teams that could add great value to those operations. Ad-Hoc networking will probably be the only way that the development of nanotechnology cooperative 'dust mites' can come to fruition; creating a managed network for so many nodes at such a small scale seems as difficult as running a cable to each of the micron sized nodes. IDS for Ad-Hoc networks is just beginning to move out of research and into practice; practices that will be of value to any Wireless IDS deployment. Ad-Hoc network Intrusion Detection may also be the approach that can be leveraged by the home user. While personal firewalls have taken some time to reach most consumers, the technology has become such a recognized asset that Microsoft and Apple have begun building firewalls that are closed by default into their operating systems. Once cooperative or node based WIDS matures it will undoubtedly replace the current posture of careless scanning and default association behaviors common to current Windows and Macintosh Operating Systems.

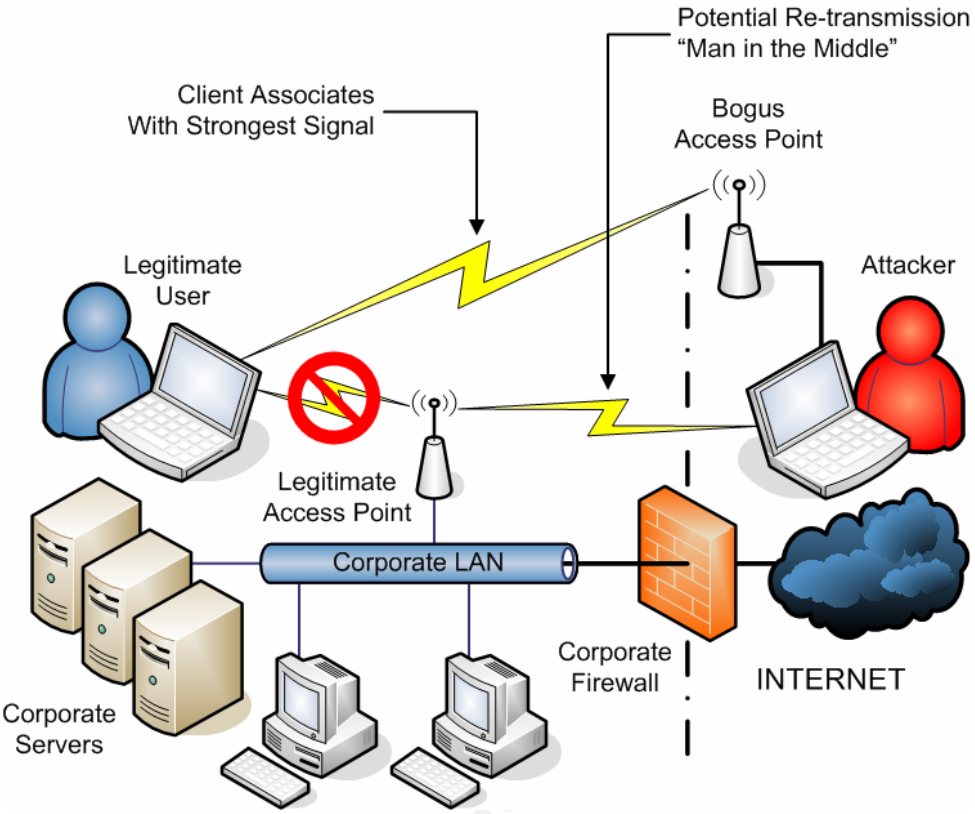

Figure 2

The Bogus Access Point is a direct attack against the Wireless Network that leverages the design of the Wireless Client adapters. Wireless clients are designed to roam through a physical space and therefore track the signal strength of the Access Point to which they are associated. As it roams a client will re-associate with the Access Point providing the strongest signal; however, there is no guarantee that the Access Point is the appropriate one with which to associate. [Figure 2] Discovering the Service Set Identifier [SSID] of a WLAN requires the capture of only a few packets and the wireless client will associate with the Bogus Access Point even if it cannot authenticate. While this could be a simple denial of service as the client can no longer access the network, there are greater threats if the attacker remains undiscovered. If the client can authenticate with the Bogus Access Point, then other network credentials or confidential data may be transmitted directly to the attacker in addition to plain text documents and other normal traffic. It is possible that the attacker could redirect traffic into the network after adding malicious payloads to the packets, creating new avenues into the heart of the LAN. The Bogus Access Point can only be detected, it can not be prevented. Some network plans include placing the approved Access Points as far inside the building as possible to try to minimize the signal bleeding into public, but there are many ways to amplify the strength of both receiver and transmitter. So in and of itself a wide perimeter is little protection against a determined adversary; professionals can't really expect the bad guys to worry about FCC limits on RF transmission signal strength.

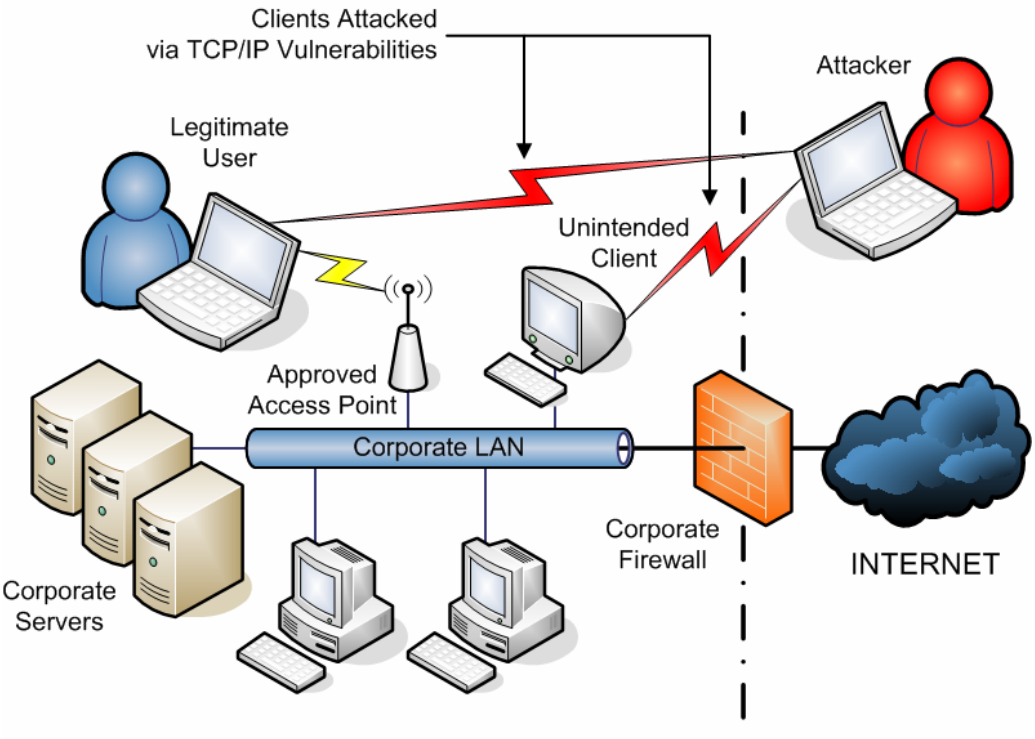

Figure 3

Approved Access Points and clients are also vulnerable, even if efforts have been made to secure the hardware and connections. Wireless Clients are still vulnerable to TCP/IP based attacks but now the physical dimension spreads the location from which the attack can be launched to the parking lot, the street outside a building, and given sufficient transmission strength, some location across and down the street. [Figure 3] The question of where an attack is coming from expands from trace routing the IP Address to searching the area in and around the location of the client being attacked. Once a client has been compromised a keystroke logger makes short work of the rest of the penetration and the event quickly escalates to complete compromise of everything that client can access. Access Points can also be suppressed or compromised, most default to exposing an HTML Administration interface to wireless clients which could allow an attacker to reconfigure the Access Point either to deny its use or to re-open closed protocols and proceed deeper into the network. Particularly troublesome are new computers that are delivered with Wi-fi enabled and unprotected; without monitoring the airspace a system administrator might not discover the intrusion until much too late in the game to do anything but clean up. Windows platforms in particular scan the entire 2.4GHz spectrum announcing their presence and requesting connections, which they will accept from anyone. Even configuring a Windows client to only associate with managed Access Points will not prevent the scan of the entire spectrum or the roaming requests. Given Microsoft's eventual shift to including a personal firewall in its operating system and then finally, with Service Pack 2, making the default configuration blocking incoming connections, sometime in the future Windows products may no longer exhibit this behavior. That is not to exonerate Apple whose Airport enabled computers are delivered with wireless networking enabled, although Apple does seem to be able to address some vulnerabilities with a bit more speed and determination than Microsoft.

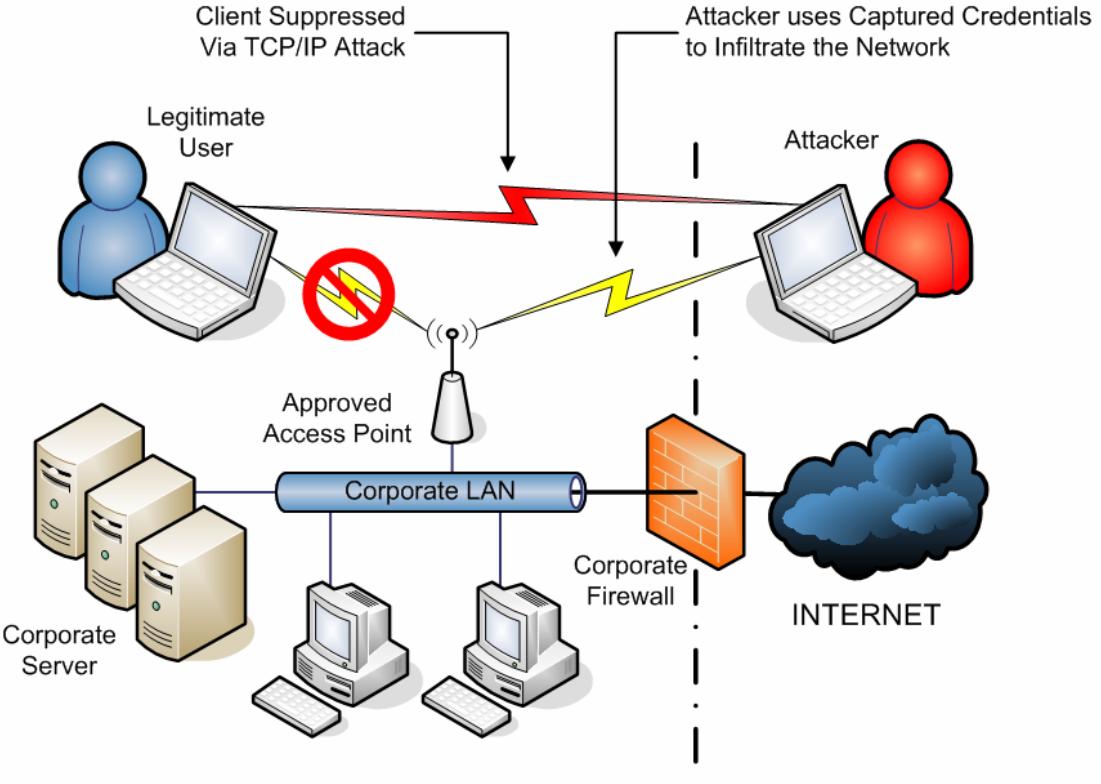

Figure 4

A Wireless Client could also be mimicked closely enough to add new life to the Mitnick or 'Man in the Middle' Attack. If enough data had been collected to effect a 'replay' type association or compromise the client's credentials, then an attacker would only have to suppress the legitimate client and re-associate with the Access Point to gain entry to the network. Masquerading as the legitimate client, the attacker could then elevate privileges or peruse the network deciding where to go next. [Figure 4] Unless the client computer was protected with a node level firewall, like Zone Alarm or Black ICE, it would be unable to prevent being suppressed or report its condition to a central server. Ad-Hoc or larger networks might never discover a compromise as nodes are expected to roam in and out of the network, while the other nodes adjust their routing tables to suit a continuously changing network topology.[ix] If not detected swiftly, all traces of the attacking node or compromise could be swept away as the network rearranges itself; leaving all of the other network nodes thinking that they were communicating with another, approved node.

The attack vectors created by Wireless Networking vary from easily prevented to difficult to protect against. Given enough time and/or enough data to capture the 'would be' intruder can impact any system and potential intrude into any network. Amateurs are likely to reveal their presence by their choice of tools; while expert crackers may glean enough by simple eavesdropping that they don't even see a need to intrude any farther. Wireless IDS can provide knowledge of the evolving situation by monitoring both transmitted data and activity in the Radio Frequency Spectrum, but malicious misuse of the network is probably best left to LAN IDS.

LAN and WLAN Intrusion Detection

LAN IDS is at a higher level of maturity, particularly the heuristic based systems, while Wireless IDS is just beginning to grow past its infancy. In addition to having to deal with the new media, radio frequencies, Wireless IDS systems must also have an understanding of the physical location in which they are deployed. Wireless networks are also inherently unstable; nodes are designed to be mobile, transmission strength can be affected by many factors, and the network itself is designed on the premise that most nodes will have to route through other nodes to maintain connectivity. Fragmented packets or half established TCP connections are no longer necessarily the product of a malicious attack; it could just be the node moving behind a pillar or into some other dead spot in the physical environment. A truly robust Wireless IDS would have to use either sophisticated knowledge of its local radio frequency topology or use cooperative evaluation between all of the wireless nodes on the network.

802.11 networks may or may not be connected to a fixed wire network; corporations would undoubtedly want to provide access to server assets if deploying Wi-fi within its physical space, while emergency management or response teams would probably not even consider using Access Points favoring the flexibility of a mobile, Ad-hoc network. Both Wireless Networks would require some concept of physical location; the mobile network nodes really indicate a need to integrate GPS with each node, while the Wi-fi addition to a fixed wire network could find that knowing office locations was sufficient. However, because of the lack of physical channels all wireless Intrusion Detection Systems must include some representation of their environments; there simply is no wire to follow to the compromised network node. This requirement holds even for those networks that do not intend to deploy 802.11 networking.

Any fixed wire network should to be using some combination of firewall, egress filtering, and intrusion detection to provide a baseline of network security and knowledge of normal network activity. Now, due to the wireless revolution, network managers must add at least some level of 802.11 IDS or at least RF monitoring. As has already been illustrated, simply because Wi-fi is forbidden by policy does not mean that Wi-fi will not show up on the network, even if its deployment is unintentional. If an organization has taken any measures to protect its network, then its administrators should also be protecting the airspace in and around the network. There are already several classes of products available to network administrators ranging from software tools that leverage consumer grade wireless adapters to dedicated server and detector based systems, like AirDefense [http://www.airdefense.net], to dedicated handhelds, like AirMagnet [http://www.airmagnet.com/products/handheld.htm], that allow administrators to roam around the building until signal strength leads them to the wireless node.

The use of Wireless IDS does not remove the need to deploy IDS on the fixed wire side of the network; the exception being a completely Ad-Hoc network, common to deployed networks like those being developed or in use by Emergency Management Departments around the US. If the wireless network is intended to integrate with the LAN at any point, then that LAN should have its own IDS to identify malicious behavior within the fixed wire network. Many businesses have discovered the hard way that even if roaming users only leverage Wi-fi when out of the office, at home or in an airport or coffee shop,

the roaming user has a higher likelihood of introducing a worm, virus, or other malicious code when reconnecting to the office LAN. This was true of laptop users in general before wireless networking; however, it is now far more likely because of the porous nature of the wireless medium and the number of locations that provide Internet access. 3Com has introduced a Network Interface Card that includes a node level firewall featuring an ability to use different profiles in different locations to protect users of several fixed wire networks[x]. Hopefully, 3Com will see a need to develop similarly equipped 802.11 adapters. Zone Alarm and other personal firewalls can also provide a certain amount of node protection, if the user is sufficiently technical. But so many users simply click on the 'OK' button and several recent malicious code exploits do not require user execution; the cross-scripted JavaScript attack and JPEG/GIF poisoning being two recent examples. If users will be roaming in public and then re-connecting to the office LAN, then the LAN should have its own IDS to aid in detecting Trojans and worms. Likewise, if users are using wireless within the office to connect into the fixed wire LAN, then the LAN must be protected by its own IDS.

Many of the companies that provide virus detection and other security related applications are now improving or adding product offerings for Wireless scanning and detection. Open Source tools, like Kismet [http://www.kismetwireless.net], are maturing into useful and powerful tools for system administrators. While all of these tools can sufficiently match the signatures of known exploit scripts, the heuristic, or behavior, based detection of wireless connections and compromises are still a bit too complex to adequately determine whether wireless activity is malicious or caused by RF interference. When a wireless client disappears from the network, deciding if that node is under attack and being suppressed or if that node has simply wandered into a dead spot is non-trivial. Fragmented packets and incomplete TCP handshakes could also either be due to malicious behavior or wandering into dead spots or radio interference. Microwave ovens and some other common appliances create interference in the 2.4GHz spectrum and since many are used intermittently, the interference can appear random and difficult to benchmark. Depending on the response a network team intends for potential intrusions, this approach could be adequate, however heuristic wireless analyzers will require a much longer period of baseline analysis before their false positive rate is decreased to a point where an automated response could be used reliably.

A server and detector based system deploys dedicated detectors around a physical installation, detectors that report back to a central monitoring server usually over TCP/IP. While such systems can be somewhat expensive to deploy and require that at least the Access Points be cataloged by the server, a detector/server based system can provide continuous airspace monitoring in areas where 802.11 networks will not be deployed. These systems monitor the Radio Frequencies used by Wi-fi gear examine the packet headers intercepted on those frequencies. They will reliably alarm when a new Access Point is stood up and when Wireless Clients try to establish an Ad-Hoc network. However, their ability to detect malicious behavior is questionable, if provided, and they use MAC Addresses to identify nodes. Using MAC Addresses for identification will catch amateurs but miss the skilled adversary; wireless transmissions can be received without revealing the presence of the eavesdropper and MAC Addresses are easily spoofed in the wireless environment. The detectors do not protect wireless nodes directly and in large installations the server could become difficult to manage since approved

nodes must be entered into the server's database. Additionally, wireless clients are expected to wander in and out of the air space, most of these centrally monitored systems will either not track clients or alarm as clients disappear from the network. However, in a physical location where wireless is forbidden by policy such a system can provide nearly real-time detection of wireless activities and a starting place for a detailed search using a handheld detector.

Handheld IDS detectors can be extraordinarily useful when tracking down a suspect 802.11 device. While limited in range, many do a good job of examining signal strength and azimuth providing useful information when trying to pinpoint the location of a transmitter. AirMagnet and Berkeley Varitronics Systems' Yellowjacket products [http://www.bvsystems.com/Products/WLAN/WLAN.htm] while not necessarily adequate for continuous monitoring are good choices for both tracking down suspicious nodes and surveying an area for dead spots and other anomalies. These systems can be integrated with GPS and mapping software in order to conduct surveys of the RF air space and its asymmetry, which is exceptionally useful given the importance of the physical parameter in Wireless Intrusion Detection.

Protecting Ad-Hoc Wireless Networks should be the subject of another paper since the centralized model of protection is not transferable to a network that is decentralized and created by cooperation. In an Ad-Hoc network nodes must cooperatively analyze the behavior of a peer node to determine if that node or its behavior is suspect. The nodes in an Ad-Hoc network must also be able to take action cooperatively; possibly either switching channels or authentication keys or both in order to isolate the suspicious node.[xi] However, such a cooperative approach to intrusion detection could become very useful in a managed wireless network if Access Points were treated as just another node in the network. If the nodes themselves can identify misbehavior at the MAC layer and take appropriate action while maintaining connectivity for the rest of the nodes, then the IDS would become far more robust and correct than most of the current offerings.

While there are many good products and services available for Wireless IDS, most lack the critical component of determining physical location with any real degree of certainty. Because of the inherent lack of physical security in wireless networking, being able to identify the location of a transmitter becomes an important part of the IDS puzzle. Signals coming from outside of the normal transmission space should be immediately suspect even if they conform to all other features of an approved transmission. Being able to identify whether a new Access Point is on premises or in the parking lot outside would allow the network team to instantly differentiate between Rogue and Bogus Access Points; leading to a faster response and potentially eliminating loss due to a successful penetration. Regardless, Wireless IDS must be part of a defense in depth strategy, including LAN based IDS to protect the fixed wire portion of the network as well as protecting each wireless device at the node level with a firewall.

Indicated Improvements

Wireless Intrusion Detection is beginning to evolve from covering basic attack vectors and radio frequency monitoring to advanced, heuristic and cooperative based analysis. There still remains quite a bit of work to bring improvements in the algorithmic approach to Intrusion Detection to the Wi-fi connected world, although some of the lessons learned

by Cell Phone carriers and service providers are being applied to existing tools. Research efforts are also being integrated into new IDS tools at a brisk pace, possibly rendering this paper outdated after the date of its submission. Especially in the realm of Ad-Hoc and cooperative networking, detection improvements are crucial to the success of the evolving Ubiquitous Computing environment.

Location identification using GPS, signal triangulation, or location fingerprinting will add reliable positioning of network nodes in physical space. As previously mentioned, knowing the location of a transmitter can yield large benefits in identifying malicious Wi-fi behavior. Knowledge of the typical locations from which to expect wireless transmissions could eliminate many of the vulnerabilities that exist because of signal bleed and variations in signal strength. Fingerprinting RF transmitters by the anomalies in signal profile was used by cell phone service providers to identify cloned cell phones created from transmitted A-Key phone identifiers.[xii] Developing a uniquely identifying signature for all wireless nodes could severely reduce, if not eliminate, the ability for an adversary to impersonate a legitimate node on the network. Both of these improvements will go a long way to improving the correctness of Wireless Intrusion Detection Systems' identification of intruders and responding appropriately by refusing to route traffic from that node or otherwise isolating it.

GPS locating seems an obvious choice of locating technology, however it has its own shortcomings. GPS aware devices currently require separate hardware and interfaces to utilize the satellites which can present a cost hurdle and add to the total cost of ownership. Even though the GPS service limitation for civil users was lifted in 2000, location precision is still limited to around 2 meters and requires a clear line of site to several satellites in order to maintain accuracy. Line of site into the heavens is an unlikely prospect in an office environment, while 2 meters may or may not be accurate enough for outdoor applications. Furthermore, position information would have to be included in transmission packets, which implies that the data could be easily spoofed.

Signal triangulation on signal strength by itself is problematic due to issues arising from signal reflection and refraction, intermittent interference, and assumed visibility of one node to several other nodes or access points. Triangulation relies on determining the overlap of reception in several sensors or nodes; less than three pieces of information renders triangulation useless. If the reception strengths are attenuated intermittently by either appliance interference or roaming into degraded signal areas then triangulation will yield an erroneous location for a given node. Further degradation of triangulation confidence can be caused by signal reflected or refracted off of interior surfaces distorting the originating signal's location.

A more complete locating algorithm, Location Fingerprinting, utilizes triangulation and a survey of the radio frequency interference environment in which to locate nodes. Truly robust technologies will determine signal origination by angle of arrival, time of arrival, and received signal strength weighted against entries in a database created during a full radio frequency survey of the physical environment.[xiii] The results of such analysis, if completed in real time, would then only be adversely impacted by intermittent interference like that created by microwave ovens. This is probably the most promising approach to physically locating nodes in a wireless network even though it is somewhat

computationally intensive and less reliable in large or outdoor environments as it has a sound theoretical basis and only seems to require some algorithmic tweaking to improve its performance.

Another key improvement to provable node identification is fingerprinting the anomalies of individual Wi-fi transmitters. Taking a cue from the cell phone industry, fingerprinting focuses on the transient features of a radio signal that are peculiar to each individual transmitter. The cell phone industry initially developed this approach to limit their losses due to the cloning of cell phone identification credentials, known as A-keys. The authentication tokens were being harvested by radio frequency eavesdropping and then burned into the EPROM of cloned phones, which were then frequently used in international per-fee call centers. Large amounts of money were lost as legitimate users challenged huge bills reflecting multiple calls to third world countries. Cellular service providers responded by both profiling usage and using the anomalies of each phone as an additional authentication mechanism and their losses due to fraud were greatly reduced. This reaction to fraudulent use is being applied to several emerging technologies including Toll Tickets and other RFID applications which are becoming ubiquitous enough to suffer large monetary losses due to fraud.[xiv]

A similar approach will soon be applied to verification of 802.11 nodes.[xv] By creating a database of identified 802.11 transmitters and their fingerprints, ensuring that a node has been previously approved and is not being mimicked becomes a simple matter of comparing the signal features against those previously recorded. The fingerprint of a transmitter could also be utilized as an additional authentication mechanism, since the anomalies are so difficult to spoof. The research of Jeyanthi Hall, Michel Barbeau, and Evangelos Kranakis of Carleton University, School of Computer Science is already mature enough to integrate into smaller Wi-fi networks where false negatives, i.e. legitimate nodes being refused authentication based on failure to match fingerprints, are quickly and easily addressable. They are continuing to fine tune their algorithms and will hopefully find the approach to be of interest to industrial partners. This single development could represent the largest improvement in closing the inherent vulnerabilities and detecting intruders in wireless networking for small to medium sized organizations.

These suggested improvements to the current toolset available for Wireless Intrusion Detection still do not address the issues surrounding home users and roaming users on public hot spots. Virtual Private Networks, with single use authentication tokens, can go a long way towards protecting traffic inbound to a LAN, providing that the LAN is protected by an IDS. Node level firewalls, whether centrally managed or not, will probably remain the best method for securing each node from attack for the foreseeable future. Unfortunately, using the slow adoption of personal firewalls by most consumers as a guide it would seem that naïve home users will remain exposed to malicious intruders.

Conclusion

As Wi-fi capability has become more ubiquitous in computing devices, Wireless Intrusion Detection has gained increasing importance in the pursuit of a secure networking environment. If the alarming speed at which viruses and exploit code appears

after vulnerabilities are discovered is any indication of the capability of our adversaries, then it should be ceded that intrusion via wireless networking should no longer be considered an 'if' but a 'when.' Even if forbidden by policy, new equipment being introduced onto a network can unintentionally open the LAN through embedded and, by default enabled, Wi-fi functionality. The uses, and potential abuses, of the 802.11 standard have only begun to be explored and revealed; clearly Wi-fi networking will be a part of the networked computing environment for a long time to come.

Current Wireless IDS products, both commercial and Open Source, can be used to piece together a fairly robust defense in depth security solution. There are also several companies offering either managed services and equipment or homogeneous, modular Wireless IDS. The most crucial acknowledgement must be the fact that no organization should be without some sort of radio frequency monitoring regardless of whether or not Wi-fi has been approved for networking. Consideration must also be taken for roaming users and those working from home, since those users may either inadvertently introduce malware upon reconnecting at the office or inadvertently create an opening through the network defenses via their home network. Wireless IDS products will undoubtedly proliferate in the near future; hopefully they will gain and maintain an edge on adversarial intruders.

Suggested Reading

Vladimirov, Gavrilenko, & Mikhailovsky, WI-FOO: The Secrets of Wireless Hacking. Addison-Wesley for Pearson Education, Inc. Boston, MA. 2004 ISBN: 0-321-20217

Barken, Lee, How Secure Is Your Wireless Network: Safeguarding Your Wi-fi LAN. Prentice Hall PTR, Upper Saddle River, NJ 2004 ISBN: 0-13-140206-4

Gast, Matthew S. 802.11 Wireless Networks: The Definitive Guide. O'Reilly & Associates, Inc. Sebastapol, CA. 2002 ISBN: 0-596-00183-5

Horton & Mugge, Network Security: Portable Reference [Hack Notes Series] McGraw Hill/ Osborne, Emeryville, CA 2003 ISBN: 0-07-222783-4

---

[i] Office of Information Technology. *Inadequate Security Controls Increase Risks to DHS Wireless Networks* OIG-04-27 June 2004, http://www.itvshop.com/wlan-security/dhs.pdf (2 Aug 2004)

[ii] Code of Federal Regulations. 47 C.F.R. § 64.1200(a)(7)
"(a) No person or entity may: ... (7) Use any technology to dial any telephone number for the purpose of determining whether the line is a facsimile or voice line."
http://a257.g.akamaitech.net/7/257/2422/05dec20031700/edocket.access.gpo.gov/cfr_2003/octqtr/47cfr64.1200.htm (3 Aug 2004)

[iii] Ciarcia, Steve. *Priority Interrupt*, Circuit Cellar, July 2004, Issue 168
http://www.circuitcellar.com/library/priorityinterrupt/168.htm (26 Aug 2004)

[iv] Adam, A K M. *So Weirdly Wrong*, Akma's Random Thoughts, August 22, 2004 [uncorroborated article]
Shttp://akma.disseminary.org/archives/001518.html (3 Sept 2004)

[v] Wright, Joshua *Layer 2 Analysis of WLAN Discovery Applications for Intrusion Detection.* 8 Nov 2002
http://home.jwu.edu/jwright/papers/l2-wlan-ids.pdf (2 Sept 2004)

[vi] bluejackQ with a Q, "the world's first website dedicated to bluejacking"
http://www.bluejackq.com/ (13 Sept 2004)

[vii] ConnectU-Wireless : : Wireless Intrusion Detection and Response
http://www.fullmesh.net/Products/detection.html (13 Sept 2004)

[viii] Cranite Systems, Inc. - WirelessWall Product Page
http://www.cranite.com/solutions/wirelesswall/index.php (2 Sept 2004)

[ix] P Kyasanur & N Vaidya, *Detection and Handling of MAC Layer Misbehavior in Wireless Networks* Technical report, CSL, UIUC, August 2002
http://citeseer.ist.psu.edu/kyasanur02detection.html (6 Sept 2004)

[x] 3Com® Embedded Firewall solutions – Product Offerings
http://www.3com.com/products/en_US/prodlist.jsp?tab=cat&pathtype=purchase&cat=134482&selcat=Security+Products&family=134494 (16 Sept 2004)

[xi] Y Zhang, W Lee, & Y Huang, *Intrusion Detection Techniques for Mobile Wireless Networks*. ACM Mobile Networks and Applications (MONET) Journal, 2002 , 1-16
http://citeseer.ist.psu.edu/zhang03intrusion.html (13 Sept 2004)

[xii] Veeneman, Dan, *PROTECTION AGAINST CELLULAR FRAUD*. Monitoring Times, Jan 1999
http://www.decodesystems.com/mt/99feb/ (6 Sept 2004)

[xiii] K Kaemarungsi & P Krishnamurthy, *Modeling of Indoor Positioning Systems Based on Location Fingerprinting*. IEEE INFOCOM 2004
http://citeseer.ist.psu.edu/651825.html (3 Sept 2004)

[xiv] Y Moreau, B Preneel, e. al., *Novel Techniques for Fraud Detection in Mobile Telecommunication Networks*. ACTS Mobile Summit 1996
http://citeseer.ist.psu.edu/moreau96novel.html (3 Aug 2004)

[xv] J Hall, M Barbeau, & E Kranakis, *DETECTION OF TRANSIENT IN RADIO FREQUENCY FINGERPRINTING USING SIGNAL PHASE*.
Proceedings of the 3rd IASTED International Conference on Wireless and Optical Communications, ACTA Press, Banff, 2003.
http://citeseer.ist.psu.edu/587549.html (3 Sept 2004)

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event