Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Enterprise 802.11 Security Considerations and Vendor Solutions

Enterprise wireless LAN deployments are unquestionably on the rise, driven largely by demand from employees using the technology at home. Improperly secured wireless networks provide an open gateway into corporate networks for both professional information thieves as well as casual seekers of Internet access. Because the information assets in a corporate network are typically much more valuable than those in a home network, greater attention must be paid to security. New wireless products are available on the market to...

Copyright SANS Institute
Author Retains Full Rights

AD

Enterprise 802.11 Security Considerations and Vendor Solutions

Jon Green

Version 1.4b GIAC GSEC Practical Assignment
May 4, 2004

Abstract

Enterprise wireless LAN deployments are unquestionably on the rise, driven largely by demand from employees using the technology at home. Improperly secured wireless networks provide an open gateway into corporate networks for both professional information thieves as well as casual seekers of Internet access. Because the information assets in a corporate network are typically much more valuable than those in a home network, greater attention must be paid to security. New wireless products are available on the market today that are designed to address the requirements of corporate users. These products include wireless intrusion detection system, wireless LAN access systems, and software for encryption and authentication. This paper covers major security issues inherent in enterprise wireless LAN deployments as well as some of the product features vendors are delivering to address these issues.

© SANS Institute 2004, Author retains full rights.

Introduction

As a security-conscious network manager, you listened to your vendor when you installed their new wireless LAN product – you're running 128-bit WEP for encryption and authenticating everyone who gets on the network using LEAP. You're pretty confident about your network security, and you sleep well at night. Then, one morning, you come in the office and find your entire corporate web site replaced by four words: "0wn3d by 3133+ hax0rs!" – and your auditing reveals that the attackers came in through the wireless network.

One of the truths that most wireless LAN vendors won't tell you is that wireless networks *are* less secure than wired networks. No matter what you do, putting network ports in the parking lot will potentially open doors that were not previously open. Wireless offers new flexibility and increases in productivity, but cannot be deployed at the expense of security. Understanding the threats and some of the currently available products to address those threats is a critical step in managing risk.

A Layered Model for Security

Best security practice dictates that single-method security techniques are insufficient. Encryption alone in a wireless network is not enough. Strong authentication makes things better, but doesn't solve the problem of authorization. And with a single rogue AP, a well-intentioned employee can bypass the entire enterprise security perimeter. A multi-layered approach to security, known as "defense in depth," is required to provide maximum protection against wireless threats[1]. Even if an attacker makes it through one layer, the likelihood of getting through multiple layers is very low. Components such as wireless intrusion detection and prevention, encryption, authentication, and stateful firewalls can turn those open doors in the parking lot into tightly locked doors.

The general threats to wireless LANs can be classified into seven major categories, all of which must be addressed in a secure system.

- Probing / Network Discovery
- Denial of Service (DoS) attacks
- Surveillance
- Impersonation
- Client-to-Client Intrusion
- Client-to-Network Intrusion
- Rogue APs and Ad-Hoc Networks

[1] Cole, p.11.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Network Discovery: How to Make your Network Invisible

The truth is, you can't – at least not without shutting off the power switch. And there's no point in trying, because a determined hacker will find the network anyway. Network discovery is a normal part of the 802.11 protocol, allowing clients to learn about available services – without it, legitimate users wouldn't be able to access the network. However, network discovery mechanisms also allow both war-drivers in search of free Internet access and potential attackers looking for entry to the corporate network to find targets.

Network discovery in 802.11 works in one of two ways. In *passive discovery* mode, a station simply listens for beacon transmissions coming from access points (APs). These beacon frames normally contain the SSID of the network, as well as clock synchronization data and other parameters regarding capabilities of the AP. Once a passive station detects these beacons, it displays the SSID to the user. In *active discovery* mode, on the other hand, stations actively send out messages called *probe requests* to APs in the area. These probe requests can be either broadcast, meaning they are searching for any network, or specific, looking for a pre-configured SSID. Access points should respond to probe requests with *probe response* messages[2].

In the earlier days of wireless LANs, it was suggested that an SSID operated like a shared password – only those who knew the SSID would be able to associate to the network. With the advent of wireless-aware operating systems such as Windows XP, this principle has long since become obsolete. However, some myths still persist. Some will suggest disabling transmission of SSIDs in beacon frames as a means to hide a network. In reality, this practice really does little to increase security. A war-driver running a passive network discovery tool may be discouraged by the missing SSID, but any active discovery tool, including Windows XP, will send out broadcast probe requests to learn the SSID. One can disable responses to these broadcast probe requests, but this practice again only discourages the casual Internet-seeker. In actuality, all it takes is a few minutes of sniffing the network, or a few seconds of running an active tool such as the freely-available "ESSID_Jack[3]", to learn the SSID.

Some types of network probing can be detected by modern wireless IDS systems. These systems are normally based on frame rate analysis or signature-based detection of some popular probing tools, including Netstumbler[4] and ESSID_Jack. Although these systems don't necessarily stop people from finding a network, they do give the network manager some visibility into what is happening. Of course, purely passive discovery is silent and cannot be detected by any system.

---

[2] Gast, p.115.
[3] Lynn, p.21.
[4] Wright(2), p.5.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Detecting and Thwarting DoS Attacks

The goal of a Denial of Service (DoS) attack is ultimately to prevent legitimate users from accessing the wireless LAN – either for an extended period of time, or just for a moment in order to carry out a specific attack. Wireless DoS attacks can be classified into two major categories: RF attacks and 802.11 attacks. RF attacks, or Layer 1 attacks, are typically referred to as *jamming*. They involve an attacker using some type of radio transmitter to generate noise in the 2.4GHz or 5GHz spectrum, with the end goal of disrupting all radio communication in that frequency band. 802.11 equipment is designed to operate above a certain signal-to-noise ratio, and in the presence of RF jamming will typically not be able to communicate at all. There is little that can be done to stop RF jamming, but some 802.11 systems have the ability to detect signal-to-noise ratio and notify the network manager when it drops below a certain threshold. If the jamming is only on a specific 802.11 channel, these systems also have the ability the search for a better channel. Fortunately, jamming is rare – owing both to the cost of equipment and the fact that it is illegal in most countries.

The second and more common type of DoS attack works within the 802.11 protocol framework. These types of attacks require only a laptop or PDA with a wireless NIC, meaning that equipment is readily available and inexpensive. These attacks range from floods of 802.11 *associate* frames that attempt to consume all available client slots in the AP, to 802.1x EAP handshake floods that try to overwhelm an authentication server, to the ubiquitous *deauth* attack that causes clients to drop their association with an AP.

De-auth attacks are the most effective of 802.11 DoS attacks. They exploit a weakness in the 802.11 protocol that forces stations and APs to use the source MAC address as the identifier of another 802.11 device. Frames are not authenticated – meaning that anyone can change the MAC address of their NIC card and send frames that appear to come from another device. Attackers exploit this weakness to send *deauthenticate* frames to stations that appear to come from the AP – stations respond according to the protocol requirements and drop their association to the AP. If this process is repeated enough times, stations will assume the wireless LAN is no longer available and will begin scanning for a new AP[5].

Modern wireless systems can provide a number of security features to identify and often prevent 802.11 DoS attacks. These may include:

- **RF fingerprinting** – examining the signal strength of a client device from the perspective of multiple APs. This is one method of detecting the source of attacks that involve address spoofing, such as deauth attacks.
- **Signature detection –** similar to traditional wired IDS systems, signature detection compares 802.11 frames with signatures of known attacks.

[5] Lynn, 15.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- **Frame rate anomaly detection** – often used for detecting high rates of 802.11 management frames such as *associate* frames.
- **Rate limiting for 802.11 management frames –** when the wireless IDS is integrated with the AP providing service to users, rate limiting allows the AP to limit or ignore management frame floods.
- **Detection of MAC address spoofing –** normally based on sequence number analysis. Each 802.11 frame contains a sequence number which is generated by the NIC chipset. Modification of the sequence number, even with a custom driver, is extremely difficult. When frames are seen in a wireless network with the same source MAC address but with sequence number anomalies, it is likely that one device is spoofing the MAC address of another station[6].

The net result of using these techniques is that some attacks can be prevented, while others can be logged and reported to the network manager. Reports can include such information as the time and date, the type of attack, the target of the attack, and the approximate physical location of the attack based on signal strength triangulation.

Surveillance: Guess What I Heard Today?

People will often give a credit card number or other sensitive information while talking on a cordless phone without thinking about the fact that anyone could be listening on an inexpensive Radio Shack scanner. The same problem exists in 802.11 networks – most non-IT people rarely consider the possibility of eavesdropping on their data network, but it is trivial to accomplish on an unencrypted network. Because it's difficult to control where RF waves end up, one can never be certain where 802.11 packets are heading or who is listening. Directional antennas don't solve the problem. Although they can more tightly direct the RF energy, they can never completely prevent signal leakage – a single metal file cabinet in the wrong location can bounce a signal in many different directions. The key to preventing surveillance is the use of strong encryption – although it's not possible to control who receives the signals, the data can be rendered unreadable by unauthorized parties. Three types of encryption are in wide use on wireless networks today, each with some variants: WEP, TKIP, and IPSEC. In the near future, the 802.11i standard will also provide strong encryption based on AES-CCMP.

WEP ("Wired Equivalency Privacy", NOT "Wireless Encryption Protocol" or one of the many other variations) has been around since the very first 802.11 standard. It was designed by the IEEE and makes use of the RC4 encryption algorithm – the same one used in SSL. This makes WEP small, relatively fast, and easy to implement in hardware on most wireless NICs. Unfortunately, the original design of WEP makes it vulnerable to cracking – given sufficient time and

[6] Wright (1), p. 5.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

data for analysis, a WEP key can often be discovered. From that point forward, an attacker can decrypt any data going across a wireless network. Although most modern WEP implementations are much less vulnerable to this cracking technique, numerous flaws still exist in WEP that make it unsuitable for anything other than a home network.

There are several tools in use for cracking WEP. Two of the early tools, called "AirSnort" and "WEPcrack", run under Linux and rely on collecting a sufficient number of frames that use *weak initialization vectors* to eventually derive the key. The initialization vector is part of the encryption algorithm, and a few certain patterns in the IV are known to weaken the encryption. Many modern 802.11 products will not generate packets with weak IVs, thus helping to ease the risk. However, avoiding weak IVs also reduces the number of useful IV values and increases the likelihood of IV re-use – essentially trading one problem for another. Some wireless IDS products can monitor for weak IVs being generated by devices on the network and notify the network manager of the need for a firmware upgrade.

Weak IVs are not the only problem, however. Other vulnerabilities in WEP include the lack of anti-replay protection, the lack of a cryptographically strong message integrity check, a small number of possible IV values, and the fact that the actual WEP key is used to encrypt frames, exposing it to direct attack[7]. Features of the *Robust Security Network (RSN)* specified in WPA and 802.11i are designed to overcome these weaknesses in WEP.

It is important to note that there are two different types of WEP in use. One, known as *static WEP*, requires all stations in the network to use the same encryption key. This is the least secure form of WEP because once the encryption key is discovered, full access to all data on the network is possible. Static WEP also generates the largest amount of data for analysis since the key remains the same day after day. Finally, static WEP presents a key distribution problem – because each device must be configured with the same WEP key, every device must be touched any time the key is changed (for example, because of an employee leaving the company.) A second form of WEP is known as *dynamic WEP*. In combination with 802.1x authentication, dynamic WEP allows a different key to be assigned to each user in the network, and provides for a *key rotation interval* that changes the key after a configured period of time. Dynamic WEP, while still leaving the network vulnerable to certain types of packet injection attacks, is a much safer choice than static WEP for enterprises who are not yet ready to move to the next level in encryption.

That next level is called *TKIP (Temporal Key Integrity Protocol)*. TKIP, along with 802.1x authentication, is a component of the Wi-Fi Alliance's "Wi-Fi Protected Access 1.0" (WPA 1.0) specification. TKIP is fairly new technology, and widespread driver support from vendors is not available at the time of this writing.

[7] Edney, pp. 67-101.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Microsoft has released updates for Windows XP to support WPA 1.0, and most NIC vendors have at least announced plans to support it, so WPA appears to be a viable contender to replace WEP. WPA is considered an interim standard, however – and will eventually be replaced by WPA 2.0 that will itself be based on the full 802.11i standard[8].

TKIP makes use of RC4, the same encryption algorithm used in WEP. This allows TKIP to run on the same client hardware that was previously designed for WEP. TKIP includes a number of security-enhancing features, including a longer initialization vector, per-packet key rotation, and a cryptographically based *message integrity check (MIC)* to ensure that each packet has not been modified in transit. The TKIP master key can be configured statically (known as "Pre-Shared Key TKIP or TKIP PSK") or dynamically assigned through 802.1x. Either method provides significant advances in security over WEP because the master key is used to derive other keys which are then used for the actual encryption operation. TKIP PSK (sometimes called "TKIP Personal" or "WPA Personal") still suffers from the same key distribution problem as WEP, and thus should not be seriously considered for enterprise installations.

The final type of encryption in common use on wireless LANs is IPSEC. IPSEC has been used for many years to provide everything from VPN access over the Internet to secure communication of financial transactions. Most mobile devices available today support some form of IPSEC, including Windows, MacOS, PocketPC, and PalmOS. Because IPSEC is a Layer 3 protocol and provides no encryption protection at Layer 2, some form of Layer 2 encryption should always be used in combination with IPSEC when it is used over a wireless network. Despite the weaknesses of static WEP, it is suitable for use when combined with IPSEC.

The future of WLAN encryption lies in the IEEE 802.11i specification. The main difference between 802.11i and WPA is the encryption algorithm: where WPA uses TKIP (based on RC4), 802.11i mandates the use of AES (Advanced Encryption Standard). AES provides much stronger encryption than either WEP or TKIP, and is the successor to Triple-DES as the de-facto encryption type used by non-classified systems in the US Government. The downside of 802.11i is that most of the current 802.11 NICs in use today implement RC4 in hardware, but cannot run AES. That means either buying new NICs for everyone, or running AES in software on the host device. Either way, AES will represent a significant upgrade effort on the client side.

Impersonation

On a traditional wired network, figuring out who is at the end of a cable is not that difficult. Physical access to the building can be secured, 802.1x authentication can be deployed on every port, and MAC addresses can even be locked to

[8] Edney, pp. 104-107.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

physical ports. But in a wireless network, there is no "end of the cable". The endpoint of the communication is a MAC address, and as discussed above, MAC addresses can be forged. What happens if a user authenticates to the network, then has their MAC address hijacked? Will the network infrastructure treat the hijacker as an authenticated user? What happens if an attacker impersonates an AP in the network? Will legitimate clients treat the intruder AP as valid?

In many cases, solving the surveillance problem also solves the impersonation problem – if an attacker does not know the encryption key, he cannot participate in the network. However, modern wireless systems can provides an important extra layer of protection against client impersonation in the event that the encryption key is compromised. Features including sequence number analysis, de-auth attack detection, and RF fingerprinting can all work together to identify and shut down client impersonation attacks.

Another class of impersonation involves the man-in-the-middle attack. In this type of attack, an intruder causes a legitimate client to connect to an intruder's AP, then the intruder connects to the valid enterprise AP. All communication between the legitimate client and the network now flows through the attacker – allowing him to modify data, delete data, or insert data[9]. This attack again depends to a large degree on a compromised encryption protocol, so solving the surveillance problem also solves this one. Some wireless IDS products can detect man-in-the-middle attacks in progress, and if the IDS is part of the wireless infrastructure can actually prevent the attack from being successful[10].

A third class of impersonation attack involves an attacker pretending to be a valid enterprise access point, advertising an enterprise SSID. A typical wireless client machine will scan for the best AP and associate with it – and that AP could be sitting in the parking lot with a 500mW amplifier attached to it. Once a client has associated with an attacker's AP, a number of attacks can be carried out, including stealing authentication credentials, worm and virus transmission, or emulation of enterprise services for the purpose of stealing passwords. The use of properly-configured 802.1x can mitigate this sort of attack, since the AP will need to authenticate itself to the client using a trusted certificate. However, some products provide additional protection by monitoring the RF environment for unauthorized APs advertising the corporate ESSID.

Hacking other Clients: Soft and Chewy on the Inside

One of the common mistakes network managers often make with respect to security is known as "Hard on the outside, soft and chewy on the inside."[11] While spending hours on securing the network perimeter with components such as firewalls and VPN concentrators, network managers often spend little time on internal security. The "soft and chewy" part is often the individual laptop PC –

[9] Wright (3), pp. 12-14.
[10] Aruba Wireless Networks, p. 2.
[11] Johansson, p. 5.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

add a wireless NIC, and the soft and chewy part has just moved outside the network perimeter where anyone can take a bite.

Picture an attack that goes something like this: A corporate wireless network is running static WEP, and an attacker manages to obtain the key – perhaps it's an ex-employee who used to have a legitimate need for that information. The attacker associates to the wireless network, sets up a DHCP and DNS server, and starts serving out IP addresses to clients. Because the attacker now controls DNS lookups for those clients, he can redirect websites, email, or any other application that relies on DNS. Imagine that a user opens a web browser that has a default homepage set to "http://intranet" – the attacker redirects that to his own website, where the user is prompted for their username and password. With this simple exploit, an attacker is likely to obtain several usernames and passwords without ever getting inside the network perimeter.

Sometimes the attack doesn't even happen at the home office. During 2003 alone, there were a number of well-publicized Internet worms and viruses that were able to install themselves on Windows PCs and execute arbitrary code. These pieces of malicious code did everything from sending out email floods to giving full control of the machine to a remote attacker. Many times, all these attacks needed were an IP network between them and the victim. If a company has users who travel with laptops, or users who don't keep operating system patches up to date, these same risks apply. These vulnerabilities are not unique to wireless devices, but the threat is worse because of the widespread use of public "hotspots". What makes wireless users particularly vulnerable is that if their laptops become remote-controlled "drones", the point of control could be the parking lot rather than an Internet connection going through a corporate firewall.

Because wireless clients are generally more vulnerable to attacks than wired clients, it is critical to provide an extra layer of security when these clients access the network. Firewalls are the answer here. By applying identity-based firewalls to wireless users, based on that user's access rights in the network, much greater control can be exercised over what that user is able to do. For example, do traveling sales employees need access to servers containing financial documents and materials for the upcoming merger announcement? Probably not. Likewise, do R&D employees need access to sales forecasts and discount structures? Probably not. The average enterprise wired network gives equal access to every station that plugs into it, because historically it was difficult to provide authentication *and* authorization on every wired port. With modern wireless products, this limitation no longer exists. It is doubly important to provide this layer of protection for wireless users – both to protect the network from the users and to protect the users from each other.

The DHCP attack described above could be stopped with a simple firewall policy that allows DHCP packets only between the user and one or two specific servers – any DHCP packets between wireless users would be blocked. Other firewall

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

policies could be defined to allow only IP traffic, to allow email traffic only to specific servers, and to allow DNS queries only to specific DNS servers. In addition, wireless intrusion detection features such as sequence number analysis, de-auth attack detection, and signature recognition can alert the network manager when an attack on the network is underway. While measures such as these may seem overly-paranoid for the wired network, they are a necessary precaution in the wireless world.

Client remediation services are another line of defense against intrusion. This service consists of both a client-based application and a network-based service. When a user connects to the wireless network, the client remediation software will ensure that the client has virus scanning software operational and up to date, operating system patches applied, and a number of other administrator-defined parameters satisfied – all before the user is granted access to the network. Users who do not meet administrator-defined criteria will be redirected to a website where the appropriate updates can be applied.

Enterprise Network Intrusion: Storming the Castle

While a hacker's end goal may be taking control of a single client, it is more likely that he or she intends to breach the larger enterprise network. Use of the multi-layer security approach discussed in this paper - including strong authentication, strong encryption, and firewalls - will take care of the majority of potential wireless threats. However, if an intruder somehow manages to get past these multiple layers of security, the game is not necessarily over. Wireless security must be one piece of the overall enterprise security program. Network managers should plan for the worst and put into place appropriate security measures such as wired-side IDS, host-based security, internal auditing tools, and an incident response plan to handle cases when perimeter defense – wireless or otherwise – fails[12].

Rogue APs: An Intruder's Best Friend

There is no greater threat to enterprise network security today than that of rogue access points. One employee with a $50 access point from a home electronics store can single-handedly bypass the *entire* security perimeter, allowing anyone with a laptop and a wireless card free access to the internal network – without anyone knowing about it. Installing a system to *automatically* find and disable these rogue APs is an essential part of any security strategy – especially for enterprises choosing not to deploy wireless at all. This threat is real. A simple search on the Internet will reveal databases containing thousands of open access points in cities around the world that have been collected by war-drivers. While such databases are often used simply to obtain free Internet access, they also provide an easy starting point for more malicious hackers.

[12] Cole, pp. 67, 113.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

When it comes to identifying rogue APs, there are two varieties of wireless IDS products: those that can automatically classify a particular AP as rogue, and those that do not[13]. Systems that classify are able to automatically determine if an AP seen over the air is actually connected to the wired network. One method of classification involves examining MAC addresses from both the wireless and wired networks. When a match is found, it indicates a connection between the two networks. Another method of classification involves having the IDS act like a wireless client and associate to the suspect AP. If it does this and is able to communicate back to itself over IP, the suspect AP can be classified as rogue. In general, the MAC address comparison method is the better method, because it works even if encryption is used on the rogue AP. Once an AP is determined to be a real rogue AP, as opposed to an AP in a neighboring office, the IDS system can often disable the rogue AP using a simple de-auth DoS attack. Such systems can often pinpoint the location of the rogue AP on a map through techniques such as signal strength triangulation and RF fingerprinting.

Less sophisticated IDS systems flag everything seen over the air as “rogue” and leave the task of sorting everything out to a human. This type of system is not extremely useful, since the number of false positives will keep the network manager running around searching for APs so much that he will eventually disable the feature and just hope for the best.

Another class of “rogue” is the ad-hoc network. These are wireless LANs operating only between clients, with no AP in the middle. Ad-hoc networks are dangerous because anyone can join them – there is no authentication required, and often no encryption is used. If a member of an ad-hoc network is also connected to the wired network, and bridging between interfaces has been enabled, the ad-hoc network is no different than a rogue AP. Even if no bridging is taking place, users are likely exchanging data over the ad-hoc network – data that is vulnerable to surveillance. IDS products that can automatically detect ad-hoc wireless networks and wireless bridges, notify the network manager of their existence, and then provide their location on a map of the building can be effective in reducing their risk. Some IDS products also have the capability to disrupt ad-hoc networks through DoS attacks.

Now What?

There are four main points to remember when considering enterprise 802.11 deployments:

1. The technology exists today to deploy wireless LANs in a secure and manageable way. There is no excuse for sacrificing security in the name of convenience.

[13] Lindeman, pp. 1-4.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

2. Rogue APs are real. Do not underestimate the severity of threat that these represent to enterprise network security.
3. Individual clients are the most overlooked aspect of network security. Make sure that operating system patches are applied regularly, particularly to wireless-enabled clients.
4. All external connections must go through a firewall. Wireless represents an external connection. Therefore, firewalls are mandatory in a wireless network.

Even if an enterprise makes the decision not to deploy wireless networks today, these are still issues a network manager needs to be concerned with. If the IT department doesn't deploy wireless, some of the employees will – and they haven't read this paper. If the IT department does deploy wireless, a layered approach to security is absolutely essential. Skip one layer, and the network is vulnerable. Skip multiple layers, and the network could be wide open to attackers.

© SANS Institute 2004, Author retains full rights.

References

Aruba Wireless Networks. "Enterprise RF Security." Oct 2003. URL: http://www.arubanetworks.com/pdf/RF-Security.pdf (21 Nov 2003).

Bellardo, John and Stefan Savage. "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions." 16 May 2003. URL: http://ramp.ucsd.edu/~bellardo/pubs/usenix-sec03-80211dos-html/ (21 Nov 2003).

Cole, Eric et al. SANS Security Essentials: Defense In-Depth. United States: SANS Institute, 2003.

Edney, Jon and William A. Arbaugh. Real 802.11 Security: Wi-Fi Protected Access and 802.11i. Boston: Addison-Wesley, 2004.

Gast, Matthew. 802.11 Wireless Networks. Sebastopol: O'Reilly & Associates, Inc., 2002.

Lindeman, Jesse and Frank Bulk. "WLAN Security Monitors: Watching the Waves." Network Computing, 4 Mar 2004. URL: http://www.nwc.com/showArticle.jhtml?articleID=18200309 (1 May 2004).

Johansson, Jesper. "Anatomy of a Windows Hack." Microsoft Corporation. URL: http://www.nexus.se/events/files/Internet_security.pdf. (1 May 2004).

Lynn, Mike and Robert Baird. "Advanced 802.11 Attack." 31 Jul 2002. URL: http://www.blackhat.com/presentations/bh-usa-02/baird-lynn/bh-us-02-lynn-802.11attack.ppt (21 Nov 2003).

Wright, Joshua. "Detecting Wireless LAN MAC Address Spoofing." 21 Jan 2003. URL: http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf (21 Nov 2003).

Wright, Joshua. "Layer 2 Analysis of WLAN Discovery Applications for Intrusion Detection." 8 Nov 2002. URL: http://home.jwu.edu/jwright/papers/l2-wlan-ids.pdf (21 Nov 2003).

Wright, Joshua. "Top 3 Attack Tools Threatening Wireless LANs." SANS Webcast. Mar 2003. URL: http://www.sans.org/webcasts/access.php?id=90446&pid=1319373151 (21 Nov 2003).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: September 2nd, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced