



## **Wireless Intrusion Detection**

*Dr. Joshua Lackey, PhD*  
*Andrew Roths*  
*Jim Goddard, CISSP*

---

## Contents

---

- 1 Overview of WLANs**
- 3 Common Wireless Attacks and Exploit Tools**
- 5 Wireless Intrusion Detection Prototype**
- 9 Incident Management**
- 11 Future Development**
- 13 Conclusions**
- 14 Summary**

### Introduction

Wireless local area networks (WLANs) continue to grow rapidly despite sluggish capital spending and overall poor economic conditions. One study conducted by the Synergy Group in Phoenix, Arizona showed that WLAN equipment sales rose to \$450M in the first quarter of 2002. This was a 55% increase from the first quarter of 2001.<sup>1</sup> Possibly driven by the low entry cost of wireless networks and the relative ease of use, organizations seem to be inclined to invest capital dollars in wireless networks as opposed to traditional LANs.

The advent of WLANs, however, has opened organizations up to new IT security threats, and many traditional countermeasures are ineffective in dealing with them. Wireless access to networks, for example, cannot easily be monitored and controlled through perimeter defenses such as firewalls and proxy servers. A wireless access point may open the internal, non-protected network up to unknown and non-trusted users who are simply within communication range.

This paper describes a new technique for monitoring, detecting and responding to information technology security breaches that occur over a WLAN using the 802.11 protocol. Advanced research at IBM Global Services has provided a working prototype of an intrusion detection system that can detect and respond to common wireless attacks that have the potential of compromising an organization's information confidentiality, integrity and availability. This research has also shown a methodology for automating configuration management verification of an organization's wireless access points. This is a key component to an intrusion detection system as improperly configured access points are perhaps the most dangerous risk for the WLAN.

### Overview of WLANs

The most popular wireless local area networks communicate with a layer 1 and 2 type protocol specified by the Institute of Electrical and Electronics Engineers (IEEE) 802.11 Working Group. There are various amendments to this specification which increase communication speed by changing the modulation and/or the frequency band. These enhancements are called 802.11b, 802.11a, and 802.11g. Ultimately, these protocols are extremely similar to the IEEE 802.3 standard for Ethernet or traditional wired networks. So similar, in fact, that one often forgets that there are key differences.

---

---

## Highlights

---

---

***In a wireless network, however, one cannot make the assumption that wireless users are trusted.***

In traditional networks, a user plugs into a network using some form of cabling such as coaxial, category 5, or fiber optic. He might then communicate with a Dynamic Host Configuration Protocol (DHCP) server to obtain an IP address to begin communicating with other systems. In this case, the user is assumed to be trusted since he has physical access to the port that is normally in a security-enhanced office environment. While 802.1x port-based network access control may be used before communication is allowed, these methods are rarely employed on a wired network.

In a wireless network, however, one cannot make the assumption that wireless users are trusted. Malicious individuals could easily sit outside an organization's premises and, if allowed, freely connect to a wireless network. A mechanism was provided in the protocol to require wireless clients to first authenticate with a wireless access point (WAP) before they are allowed to conduct further communications. Here, at the wireless access point, all the defenses are at one choke point. It is critical for the access point to properly authenticate a wireless client to verify that only authorized users are given access into the organization's network. One should note that in normal WLAN deployments, a wireless access point will also be connected to the internal network, so once a user is authenticated by the WAP, he will have as much privilege to internal systems as a user on the physical network.

The most common method to authenticate users involves the Wired Equivalent Privacy (WEP) protocol. This is essentially a symmetric key encryption method that requires a user to know the common key for the access point. The most common encryption algorithm used with WEP is RSA Security's RC4 algorithm.

Much as on the wired side, 802.1x authentication is available. This is generally provided by an optional 802.1x security feature called EAP (Extensible Authentication Protocol) or Cisco Systems' LEAP (Lightweight Extensible Authentication Protocol) where Lightweight implies the authentication is handled by the wireless device's firmware rather than the client's operating system. 802.1x with EAP is essentially WEP with dynamic per-client keys.

---

Highlights

---

***The key for wireless security countermeasures then is to help prevent unauthorized access to the WAPs that an organization may have.***

The key for wireless security countermeasures then is to help prevent unauthorized access to the WAPs that an organization may have. In so doing, the security system must also help monitor the organization's network for unauthorized or improperly configured access points as these present the greatest chance that an attempted intrusion will succeed. Before describing this system, however, it is instructive to illustrate some common attacks and exploit tools that are possible on 802.11 networks.

**Common Wireless Attacks and Exploit Tools**

A major weakness with WEP was documented in the Fluhrer, Mantin and Shamir paper "Weaknesses in the Key Scheduling Algorithm of RC-4." This weakness deals with a flaw in the RC-4 implementation that allows a passive user to sniff wireless traffic and brute force the WEP key in a short period of time.<sup>2</sup> Two tools of choice that automate this attack are WEPCrack (<http://wepcrack.sourceforge.net/>) and Aircsnort (<http://airsnort.shmoo.com/>). Regardless of the key strength, these tools make the task of sniffing and using brute force to recover a WEP key trivial. Once an attacker is in possession of a WEP key, he will be provided access to the WAP and anything to which it is connected. In a large WLAN with multiple access points, clients will find the remediation of such an attack very costly. After a key is disclosed, an organization will need to reconfigure all WAPs and clients that use this key.

Another common attack is Media Access Control (MAC) address masquerading. In this attack, malicious wireless users sniff traffic to determine MAC addresses that are being allowed access to a wireless network. Since most WAPs allow for this primitive type of authentication, once the attacker uncovers a validated MAC address, he can simply change his own MAC address using ifconfig under Linux or Control Manager under Microsoft® Windows® to change his MAC to that of the validated user. The attacker can then receive access to a WAP that is only concerned with authenticating MAC addresses. This attack only requires a wireless sniffer such as Aircsnort. Because of the simplicity to circumvent, MAC-based authentication is never suggested.

---

Highlights

---

***Yet another attack and possibly one of the most insidious types is WAP masquerading, often called man-in-the-middle. In this attack, a malicious user sets himself up to be an access point.***

Yet another attack and possibly one of the most insidious types is WAP masquerading, often called man-in-the-middle. In this attack, a malicious user sets himself up to be an access point. Users authenticate to him instead of to the appropriate access point, so the attacker now has complete control of their communications not to mention authentication information later required for access to authorized WAPs. Tools such as FakeAP (<http://www.blackalchemy.to/project/fakeap/>) provide an automated method of setting up such WAPs and are advanced enough to alter transmit signal strength and MAC addresses to make numerous WAPs appear valid. An excellent source for information on this form of attack can be found at <http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf>.<sup>3</sup> Moreover, this attack is particularly effective against machines that have wireless capability unknown to the owner. The default action is generally to associate with any WAP in range and to immediately request an address via DHCP. In this case, the machine is most likely already attached to the internal wired network and hence it becomes a bridge for the attacker's traffic.

One must not forget about common denial of service (DOS) attacks on WAPs. Flooding WAPs with nonsense traffic is easy to do. Such attacks may also adversely affect monitoring and logging that an organization may be doing with wireless traffic, and the impacts of a network relying on wireless access points can be severe.

***Finally, improperly configured access points provide the greatest risk to an organization's wireless security. WAPs do not come configured with authentication, and an access point's low price, which may be well below the minimum limit for capitalized assets, makes centralized configuration control extremely difficult.***

Finally, improperly configured access points provide the greatest risk to an organization's wireless security. WAPs do not come configured with authentication, and an access point's low price, which may be well below the minimum limit for capitalized assets, makes centralized configuration control extremely difficult. Business units will set up distributed access points without the knowledge of a central IT group, and these "rogue" WAPs will have a high likelihood of being improperly configured. Such improperly configured WAPs allow an attacker to essentially walk into an internal network much like an open, unlocked door allows anyone to walk into an office undetected. This example points out the continuing importance of the biggest risk to security—people not following the rules or using good judgment.

---

Highlights

---

***The focus on the wireless intrusion detection prototype was to provide functionality without ever specifying policy. Thus modularity was the watchword at all stages. The prototype consists of three core components: the sensor, the analysis master, and the alert adapter.***

**Wireless Intrusion Detection Prototype**

Based on the above-referenced research performed by IBM Global Services, techniques are available that can assist clients in preventing or mitigating such attacks. Of course, technology only supplements an organization attempting to protect itself. It is the organization itself and its members that prevent attacks and foster a security-rich environment, not the supporting technology. This paper describes a common architecture for monitoring wireless networks. This is the first step in performing the necessary analysis to help detect malicious activity. The paper will then describe a software approach to the analysis of data that will assist in detection of security breaches related to 802.11. Since much of this architecture is similar in design to traditional intrusion detection and vulnerability assessment topologies, we will call this overall solution a wireless intrusion detection prototype.

**Prototype Architecture**

The focus on the prototype was to provide functionality without ever specifying policy. Thus modularity was the watchword at all stages. The prototype consists of three core components: the sensor, the analysis master, and the alert adapter.

The first step in monitoring wireless traffic is to deploy sensors within a given infrastructure that have the capability of listening to, logging and forwarding wireless packets. In fact, the only requirement for a sensor is that it can receive all wireless data and that it can forward that data. Thus a sensor may simply be a WAP itself (albeit slightly modified). We have further developed code so that many modern operating systems that support wireless devices (and which have appropriately modified hardware drivers so that promiscuous or “monitor” mode can be enabled) can act as a sensor with comparable levels of reliability. Most conveniently this will be a Linux system with Personal Computer Memory Card International Association (PCMCIA) support but many other proprietary systems, such as AIX®, Sun Solaris®, or even Microsoft® Windows®, would work. With current technology, this is a simple task using small devices such as the HP iPAQ or similar devices that can run Linux. The iPAQ is particularly convenient because of its small size and Linux support, (<http://hp.com> and <http://www.handhelds.org>.)

---

Highlights

---

The sensor will require two network adapters, one wireless and one Ethernet. The wireless adapter will require the ability to place it in promiscuous mode so that it can see all 802.11 traffic. Most wireless adapters have this functionality but it sometimes requires modifications to the operating system driver to enable. There are public drivers that enable promiscuous, or “monitor”, mode including Cisco’s Aironet and Lucent Technologies’ Orinoco cards. Our prototype implementation currently supports the 802.11b Cisco Aironet, but hardware support on a Linux device is handled by modules so that Prism2-based chipset support, such as for Lucent Technologies’ Orinoco, and 802.11a and 802.11g support can be provided with a minimum of code. The Ethernet adapter, likewise, will plug into a traditional cabled network and will help provide a security-enhanced command interface to forward wireless packets and allow for administration.

***Since “rogue” access points may appear anywhere within an organization, it will be necessary to provide comprehensive coverage to a physical infrastructure such as a building.***

***Whereas traditional network based intrusion detection appliances range in price from \$5000-\$15,000, the wireless sensor must have a cost point similar to WAPs themselves - somewhere around \$200-\$500.***

Since “rogue” access points may appear anywhere within an organization, it will be necessary to provide comprehensive coverage to a physical infrastructure such as a building. Line-of-sight limitations, as well as attenuation caused with the high frequency band of 802.11, will make it necessary to deploy a large number of wireless sensors for large infrastructures. This can be mitigated through the use of special antennas, but in the end it is still necessary to deploy far more wireless sensors than one would with traditional intrusion detection devices. For this reason it is critical to deploy the lowest cost wireless sensor possible. Whereas traditional network based intrusion detection appliances range in price from \$5000-\$15,000, the wireless sensor must have a cost point similar to WAPs themselves – somewhere around \$200-\$500. Our focus has not been on which hardware to require, but more on allowing our software to run on various hardware platforms. As less expensive hardware becomes available, the wireless intrusion detection prototype can be ported with nominal effort.

---

## Highlights

---

Once a physical infrastructure has comprehensive coverage, the wireless data can now be logged and forwarded. The collection and analysis of these packets is the next step. The listening devices need to be configured to communicate encrypted information about all received packets to a centralized set of managers that will be able to conduct analysis of the data. The analysis code is capable of running on various modern operating systems and the attack detection code is implemented as loadable modules. When non-hardware based sensors (e.g., Linux sensors) are used, our prototype implementation employs the libcrypt library (<http://www.openssl.org>) to help safeguard communications between sensors and analysis masters. The prototype defense modules analyze the data and, if necessary, generate alerts. Alerts will be forwarded, again encrypted, to an operations console where the appropriate response can be determined.

In the working prototype that IBM has developed, these alerts are encrypted and delivered to the security operations center console in Boulder, Colorado. This is done in a variety of ways. Alerts can be tunneled through the Internet via a TCP tunnel, a secure version of the Internet Protocol (IPSEC), or even sent via e-mail. The alerts can also be displayed as console messages or logged to the system logger. Alerts can even be forwarded to an alphanumeric pager when desired. Again, various modern operating systems will support the alert adapter software.

***As will be seen later in this paper, without location information in the alert, it is extremely difficult to implement incident response to wireless attacks.***

One should note that a distinction between the alerts in a traditional intrusion detection system and those in a wireless one is the content of the message sent to the operations center. In a standard intrusion detection system, the exploit signature and the source IP address are critical. In a wireless intrusion detection system, the same information is also required, but in addition it is essential to have the location information of the sensor as well as the location of a WAP that is being attacked or is improperly configured. As will be seen later in this paper, without location information in the alert, it is extremely difficult to implement incident response to wireless attacks.

Another important aspect of a wireless intrusion detection system deals with the physical security of the sensor. Since these devices will be strategically placed throughout an infrastructure, it is critical to have a method of preventing tampering or theft of the sensors themselves. These devices would

---

Highlights

---

***The wireless intrusion detection prototype only attempts to detect those issues that are specifically wireless-based or situations in which the occurrence of a certain sequence of packets on a wireless network would indicate an attack yet on a wired network that same sequence would be considered innocuous.***

***Also, while wireless network-discovery methods, or WarDriving, can be completely passive, methods exist where certain types of this activity can be detected.***

***The AP module determines that all employee-only WAPs remain configured correctly, for example, with 802.1x/EAP, and that at no time do they allow unencrypted authentication.***

be considered targets of opportunity since they are small in size and quite popular as handheld PCs. Our prototype utilizes custom lockboxes that are drilled into a wall or ceiling, preferably out of reach of a standing human. These lockboxes hide the sensor in such a way that a casual passerby should not notice anything more than a metal lockbox on the wall. It will look no different than an electrical circuit breaker box.

#### **Prototype Analysis – Software Implementation**

Traditional intrusion detection systems are signature based. That is, a pattern match is run against each packet for each different attack type. If the pattern is detected, an alert is generated. As it is unnecessary to reproduce previous work each time a low-level protocol changes, it is only necessary to extend the protection to include any issues introduced by the new protocol. Thus the prototype only attempts to detect those issues that are specifically wireless-based or situations in which the occurrence of a certain sequence of packets on a wireless network would indicate an attack, yet on a wired network that same sequence would be considered innocuous. Moreover, as adequate signature based intrusion detection systems are freely available, e.g., Snort (<http://www.snort.org>), the prototype solution attempts to leverage these systems whenever practicable.

Each sensor is configured to send wireless data to its master for analysis. This master may reside on the sensor itself to conserve bandwidth or the master may reside in a central location so that correlation among multiple sensors is possible. In either case, the master is configured with a certain number of attack modules – independent programs that can be loaded individually into the master’s execution space to process data and generate alerts. This way, modules can perform a number of functions. For instance Snort support could be provided through a module, thus allowing access to a number of open-source alert signatures. The wireless prototype itself includes modules that range from configuration-based signature matching for detecting misconfigured or “rogue” access points, to anomaly based wireless denial of service (DOS) detection, to a hybrid, signature-chain method for detecting more advanced attacks such as disassociation storms and relay attacks. Also, while wireless network-discovery methods, or WarDriving, can be completely passive, methods exist where certain types of this activity can be detected. Work is currently underway on our WarDriving module.

---

**Highlights**

---

***The DOS detection module uses statistical methods on signal strengths and noise levels to determine when potential denial of service attacks are occurring.***

The most important defense module, the AP module, takes as configuration a list of access points owned by the customer. The security policy for each employee-only WAP is also included. The AP module determines that only those WAPs in its database exist and that each conforms to stated policy. When an unknown WAP appears, an alert is generated. For example, a certain number of WAPs may be provided to customer guests for e-mail access and are left relatively unprotected while the remaining company WAPs are for employee use only. The AP module determines that all employee-only WAPs remain configured correctly, for example, with 802.1x/EAP, and that at no time do they allow unencrypted authentication. We have provisions for many details within this module. For example, a “protected client” is one who has, at some time in the past, correctly authenticated to a known access point which itself is following stated security policy. If a “protected client” is ever lured over to an unknown or “rogue” access point, not only will the “rogue” access point be alerted, but also so will the fact that our client is now using this access point. In many cases, this is highly indicative to an active attack.

The DOS detection module uses statistical methods on signal strengths and noise levels to determine when potential denial of service attacks are occurring. Certain time differentials are taken, such as time between beacons, and are subjected to statistical analysis. Unlike static signature-based detection, the DOS detection module is entirely governed by anomaly detection and tuned by various constants in the configuration file.

**Incident Management**

With traditional intrusion detection, the source and destination IP addresses and the attack signature represent the critical information that an investigator will use to investigate a breach of security. Using wireless intrusion detection, however, two more pieces of information will be critical: the physical location of the attacked WAP and the physical location of the sensor that witnessed this attack. Without the physical location information, it becomes extremely difficult to respond to a breach of security.

---

Highlights

---

***Unfortunately, the vagaries of signal strength due to weather conditions and different rates of absorption for different construction materials make it extremely difficult to completely automate location-finding code.***

***Frequently though, mitigation will require the assistance of physical security – to get into locations to take down a rogue access point or to cruise the parking lot to find the malicious attacker attempting to lure “protected clients” to his false WAP.***

Unfortunately, the vagaries of signal strength due to weather conditions and different rates of absorption for different construction materials make it extremely difficult to completely automate location-finding code. The overhead required to calibrate such a system would make installation prohibitively expensive. Even if such a calibration is attempted, environmental factors can completely overwhelm any calculation. A room full of people, essentially just bags of water as far as a wireless signal is concerned, can significantly affect the quality of a wireless signal.

Hence, once an alert is generated, the incident management team will have a few options. Many times, it may be possible to mitigate the exposure without physical intervention. For example, if it is simply a misconfigured WAP, the device can be reconfigured or the network port can be disabled. Frequently though, mitigation will require the assistance of physical security – to get into locations to take down a rogue access point or to cruise the parking lot to find the malicious attacker attempting to lure “protected clients” to his false WAP. System administrators will of course not have access to these remote, possibly malicious, devices.

To assist physical security in locating wireless security exposures, our prototype implementation specifies a small list of hardware along with the necessary techniques to locate offending wireless devices. We have found that a sufficiently directed antenna, such as a 15dBi yagi, along with the program Kismet (<http://www.kismetwireless.org>) provides a satisfactory method of manual triangulation. Of course such detection will need to follow an organization’s security policies and any other organizational policies that may apply.

---

Highlights

---

***No matter what the incident management process is, it is absolutely necessary to have an around the clock operation that is able to monitor, analyze and respond to threats.***

No matter what the incident management process is, it is absolutely necessary to have an around the clock operation that is able to monitor, analyze and respond to threats. Wireless attacks may have a shorter time window than do traditional attacks. For example, traditional attacks often require a reconnaissance phase to see what systems are listening, an enumeration phase to see what services are available and vulnerable, and an attack phase to exploit these vulnerabilities. Manual analysis is often required between each phase. With a wireless attack, however, a malicious user may simply use a passive method of accessing a network or capturing data and the attack will be complete. There is only one phase of an attack in the scenario where an access point is misconfigured. Likewise, attackers may conduct a quick attack that provides the needed information to attack other parts of an infrastructure. Waiting a day before reacting is usually not a prudent option. Moreover, the possibility of actually finding the attacker in a than in a standard over-the-Internet attack. One often finds that the attacker resides in some foreign country in an Internet attack whereas, in the wireless case, the attacker may be visible from your office window.

**Future Development**

One major limitation of wireless intrusion detection is not technical in nature but rather economic. Even with the lowest possible cost point for a sensor, a \$200 price tag per device can more than double the cost of a wireless deployment. Since WAPs can cost well below \$200, organizations may choose to either disregard security or wireless in general. A lower cost point per sensor needs to be a driving goal.

One possible remedy for this is for hardware vendors to program into WAP firmware a span port that will forward all 802.11x packets to a configurable IP address. The cost for a WAP should not significantly increase, and a wireless intrusion detection architecture would then only require masters instead of sensors. Modern LAN switches often employ this technique, and traditional intrusion detection technologies utilize span ports to reduce the number of sensors required on a network. There is of course some risk that forwarded traffic can be tapped, but since it would be sent over an Ethernet network this risk is mitigated by traditional physical security controls. It is estimated that the deployment costs for a medium-sized infrastructure of 20 sensors could be reduced by as much as 80%. A reduction in cost could also take place in terms of steady state overhead since there would be fewer devices to manage. Unfortunately, the 802.11 protocol is multichanneled and a standard WAP, whose job is supporting the network infrastructure, cannot constantly take itself offline as it looks for unauthorized traffic on separate channels.

---

Highlights

---

***Coverage by a lesser number of devices, perhaps with more expensive antennas carefully aimed, could at least provide coverage over the most sensitive or easiest attacked areas.***

***Another development may be to automate reconfiguration options for WAPs.***

***It would be very difficult to explain to the local coffee shop manager why we have been keeping his clients off his WAP. An attacker might also take advantage of such a defense by spoofing a WAP and allowing a security provider to shut down the real one.***

Coverage by a lesser number of devices, perhaps with more expensive antennas carefully aimed, could at least provide coverage over the most sensitive or easiest attacked areas. One should not discount the deterrence effect if an attacker is aware that the wireless network has some sort of protection. Although it wouldn't ensure protection against a determined attacker, it could stop simple opportunists.

Another development may be to automate reconfiguration options for WAPs. Traditional intrusion detection systems have long since allowed security personnel to automate blocking of malicious IP addresses on supported firewalls. The same basic methodology could apply for wireless access points. In the event that a misconfigured access point is detected, it should be possible to reconfigure or shut it down without human intervention.

The wireless intrusion detection prototype could provide this functionality via some sort of "active defense" module which could not only reconfigure a known WAP back to the security policy when found misconfigured, but could also disallow traffic to an unknown or "rogue" access point. (Say, via a "disassociation storm.") Of course one would have to be extremely careful with such an action - only "protected clients" should be "protected" this way. It would be very difficult to explain to the local coffee shop manager why we have been keeping his clients off his WAP. An attacker might also take advantage of such a defense by spoofing a WAP and allowing a security provider to shut down the real one.

### Conclusions

WLANs will continue to grow as organizations find it more cost-effective to build out networks using 802.11 as opposed to cabling. Wireless security vulnerabilities will also keep pace with this technology. As of the time of this writing, new vulnerabilities have now been discovered in most implementations of 802.1x/EAP, the protocol meant to fix the problems in WEP.

Since the traditional perimeter defenses are inadequate for wireless networks, organizations that have an eggshell model where the internal network has no partitioned security controls will be exposed to grave risks. One wireless breach can open an organization's doors and expose all of its most valued information assets. No longer will organizations be able to rely on firewalls to provide the core of their security.

The wireless intrusion detection prototype offers a modular approach to help deal with this new threat. By offering a cost-effective and scalable solution, it can allow an organization to monitor and detect anomalous traffic. With the right incident management infrastructure, organizations have the potential to achieve a level of protection that has not previously existed.

### Summary

At the time of this writing, many new standards have been proposed to improve the state of security for wireless networks. Unfortunately, there is rarely if ever a “silver bullet” in security, so administrators should not hinge all of their hopes on the next great technological standard. Security comes in tiers and combines both technology and human elements.

As new standards emerge, so will new threats. Likewise, as WLANs become more pervasive, these threats will increase in magnitude. Customers wishing to capitalize on the benefits of wireless because of its ease of use or cost will need to consider security in each step of the deployment process. This is one such prototype solution that would provide one of these tiers to security, but make no mistake it is but one element in an overall IT security program.

For more information or to learn more out IBM Global Services, contact your IBM sales representative, or visit:

**ibm.com**/services



© Copyright IBM Corporation 2003  
IBM Corporation

IBM Global Services  
Route 100  
Somers, NY 10589  
U.S.A.

Printed in the United States of America  
04-03  
All Rights Reserved

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries or both.

Microsoft and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States, other countries or both.

Other company, product, and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

- 1 Griffith, Eric. "Synergy Sees WLAN Growth." 802.11 Planet. <http://www.80211-planet.com/news/article.php/1143771>. May 23, 2002.
- 2 Fluhrer, Scott, Mantin, Itsik, and Shamir, Adi. "Weaknesses in Key Scheduling Algorithm of RC4." [http://www.drizzle.com/~aboba/IEEE/rc4\\_ksaproc.pdf](http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf).
- 3 Wright, Joshua. "Detecting Wireless LAN MAC Address Spoofing." Technical Whitepaper. January 23, 2003.