Detecting rogue access points that endanger the maginot line of wireless authentication

Zhiqi Tao

A. B. Ruighaver

Detecting Rogue Access Points that endanger the Maginot Line of Wireless Authentication

Zhiqi Tao and A.B. Ruighaver

Department of Information System, University of Melbourne
zhiqit@pgrad.unimelb.edu.au
anthonie@unimelb.edu.au

ABSTRACT

The rapid growth in deployment of wireless networks in recent years may be an indication that many organizations believe that their system will be adequately secured by the implementation of enhanced encryption and authentication. However, in our view, the emphasis on cryptographic solutions in wireless security is repeating the history of the "Maginot Line". Potential attackers of wireless networks currently will find many ways to get access to wireless networks to compromise the confidentiality of information without the need to crack the encryption. In this paper we analyze how rogue access points threaten the security of an organization's wireless network and examine the popular approaches to defend against rogue access points. We argue that, while it is easy to detect access points, distinguishing between rogue access points and legitimate access points of the organization and of other organizations is a major problem which still needs to be solved.

Keywords

wireless, 802.11, rogue access point

INTRODUCTION

Now the cost of wireless networks has plummeted, and their reliability has greatly improved, many organizations are happy to roll out wireless Local Area Networks to either extend or supplant their wired networks. The initial problems in usability and quality of service (QoS) are no longer critical issues. Most of the wireless access points (APs) and wireless network cards on the market now provide up to 54MB or 108MB of data transmission speed and will, in most cases, work reliably straight out-of-the box. Range also seems not to be a serious problem anymore as most of the wireless cards and APs can generate an excellent signal with only their built-in antenna. Still, if necessary, the use of an external antenna can further improve the signal strength.

Although the lack of security on early wireless networks is well known, that does not seem to slow down the adoption of wireless network technology anymore. Research conducted by Webb (2003) and Yek and Bolan (2003) has demonstrated that the adoption rate of wireless LAN's in Perth, West Australia, is even faster than Moore's law (Intel 2005). Although a lack of control on signal leakage due to the improved signal strength creates a significant problem, recent improvements in the encryption protocols for wireless LAN's has generated an, in our view, an unjustified confidence in the security of wireless networks. As a result many organizations do believe that the benefits of wireless LANs will outweigh the risks.

While, for now, the implementation of the new encryption protocols seems not to have compromised the strength of these encryption protocols, encryption is still vulnerable to attacks on the end-points of the encrypted channel. If, for instance, the wireless access point of a network is compromised, or replaced by a malicious access point, the identity of the other end-point can easily be compromised. This would allow an attacker to take over the identity of a legitimate user and connect to the network as that user. No encryption can protect against such attacks and as a result the initial simple encryption protocols for wireless networks have been extended with much more complex protocols to ensure that both the network user and the wireless access point can be authenticated before a secure encrypted channel is created.

While the enormous effort spent on the development of strong encryption and authentication protocols in wireless LANs was necessary to combat the problems caused by the use of an open medium and the extensive signal leakage, the suggestion that organizations can rely solely on strong authentication protocols for the security of wireless networks is, in the authors view, a dangerous proposition. The emphasis that is placed on strong authentication, without any effort to balance this with other weaknesses in wireless security, creates the wireless equivalent of the "Maginot Line", created by France to prevent an invasion by the Germans. As is well known, the Germans just went around the Maginot line and as a result did encounter almost no resistance.

The two most important weaknesses that can be used by an attacker to circumvent the strong encryption and authentication on a wireless network are the lack of security on the laptop and other devices that are used by the end user to connect to the wireless network and the lack of security on the corporate network itself. That does not mean, however, that the Maginot line itself does not have any weaknesses. The implementation of the authentication protocols and how they are used to control access to the corporate network is complex enough that we expect that most organizations will leave some weaknesses or even holes in their wireless network access. More obvious, however, is the lack of security on most corporate laptops. If an attacker can intercept the user authentication on the laptop, or change the software that is on the laptop, strong authentication protocols are not going to help. Even easier to exploit, however, are weaknesses resulting from a lack of control in many organizations on the security configuration of both their wireless network(s) and their wired network. A single unprotected access point, either on the wireless network or directly connected to the wired network, makes it easy enough to bypass the security controls and the attacker does not even have to be close to the organization.

In this paper, we will concentrate on analyzing the impact of rogue access points on wireless network security. Although widely used, we find that the term rogue access point presents a problem because of its ambiguity: Different papers (Luo,H. and Henry,P. 2003) (Bahl,P., Venkatachary,S. and Balachandran,A., 2001) (Beyah,R., Kangude, S., Yu,G., Strickland,B. and Copeland,J., 2004) (Schmoyer,T.R., Lim, Y.X.,and Owen,H.L., 2004) have used the term differently. In the end we believe that almost any kind of access point that threatens the security of wireless networks can be classified as a rogue access point, even though each may exist because of a different reason and may have a different impact on wireless security. We therefore use the term rogue access point in its most general form and will define our own, more specific, terminology for the different kind of rogue access points.

THE EVOLUTION OF WIRELESS AUTHENTICATION PROTOCOLS

Wireless networks based on IEEE 802.11 protocols have been constantly evolving in recent years. If we compare 801.11g with 801.11b, usability and quality of service (QoS) have improved, while from a security point of view Wi-Fi protected access (WPA) mitigates many vulnerabilities which existed in wired equivalent privacy (WEP).

The most important enhancement of WPA over WEP is in terms of authentication and access control. By adopting IEEE 801.1X, WPA enforces the extensible authentication protocol (EAP) based authentication (IEEE Std 802.1X 2001). This standard adds one extra component special for authentication, Remote Authentication Dial-In User Service (RADIUS). Figure 1 shows that during the establishment of association between clients and access points, the authentication frames are exchanged between clients and RADIUS server and the access point only acts as the middleman or relay (Baek,K.H., Smith,S.W. and Kotz,D., 2004) (Wong,S., 2003).

Although IEEE 802.1X was designed for mutual authentication, the implementation of it in wireless networks might still be a problem since EAP does not specify the authentication method (Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J. & Levkowetz, Ed., 2004). Research from (Mishra,A. and Arbaugh,W.A, 2002) has identified several authentication methods, such as EAP MD5, that would allow mutual authentication to be compromised. They argue, therefore, that session hijacking and Man-In-the-Middle can still be a problem in wireless networks that adopt IEEE 802.1X. However, we do agree with the industry response (Cisco System Inc., 2002), which claims that mutual authentication has been properly designed in EAP Cisco or EAP-TLS via dynamic, per-user, session-based WEP keys.

It is important to realise, however, that the mutual authentication in IEEE 802.1X authenticates the access server, not the access point. It does not prevent an attacker from setting up a rogue access point for a man-in-the-middle attack; it only prevents the use of that rogue access point for a man-in-the middle attack on the IEEE 802.1X protocol. If, for instance, the network stack of the client is not correctly configured to only allow traffic on the authenticated and encrypted channel, it may still be possible for the rogue access point to attack the client. It may even be possible for the client to be compromised before the authentication takes place.

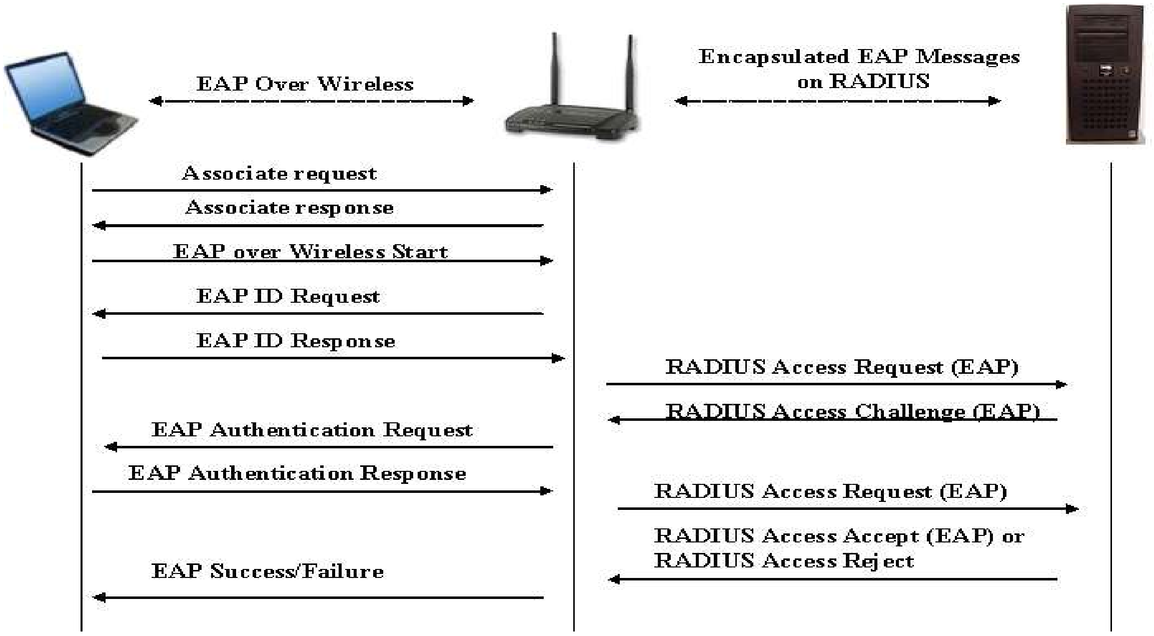
EAP Over Wireless
Encapsulated EAP Messages on RADIUS
Associate request
Associate response
EAP over Wireless Start
EAP ID Request
EAP ID Response
RADIUS Access Request (EAP)
RADIUS Access Challenge (EAP)
EAP Authentication Request
EAP Authentication Response
RADIUS Access Request (EAP)
RADIUS Access Accept (EAP) or RADIUS Access Reject
EAP Success/Failure

Figure 1: EAP authentication of client using RADIUS Access Server according to IEEE 802.1X (IEEE 2001) (Phifer 2003)

CATEGORIZING ROGUE ACCESS POINTS

Most wireless devices, such as access points and wireless network cards, have been designed with extreme flexibility in mind. Almost every characteristic of their function is software changeable including the media access control (MAC) address. Although this feature will probably improve usability in some cases, it also makes the resulting wireless networks a potential hotbed for rogue access points.

As there will be no 100% prevention, defense against rogue access points will have to include an approach based on detection and reaction. Hence, to prevent an attacker from using a rogue access point to bypass wireless authentication, they need to be detected, preferably before they are used in an attack. However, if the detection is not reliable, it may be difficult to react to the detection of rogue access points. Before we can analyze the problems in the detection of the different kinds of rogue access points, we will first need to discuss what kinds of rogue access points we expect to find.

The most common rogue access points to be found in an organization are legal access points that for some reason have not been configured properly. These are referred to as open access points (Figure 2), as the lack of security on those access points may allow open access to the wireless network. Depending on the architecture of the wireless network, an open access point may provide full or limited access to the systems on the wired network and might also be used to attack end-users connected to other access points. Hence, to limit the impact of an open access point it is important that the network architecture is correctly designed and implemented. Still, a number of so called Intrusion Prevention Systems (Airmagnet 2005) (Airdefense 2005) (Proxim 2005) are on the market, which can be used by an organization to detect open access points.

A much more dangerous form of rogue access point are those which are directly connected to the wired network, completely bypassing any security measures between the organization’s wireless network and its wired network. These are labeled backdoor access points. Backdoor access points are often setup by the personnel inside the organization for their own convenience, and may have incomplete or no security configuration enabled. A backdoor access point, however, may also be malicious and planted by a physical intruder. They can hide themselves by using a fake MAC address of an existing AP.

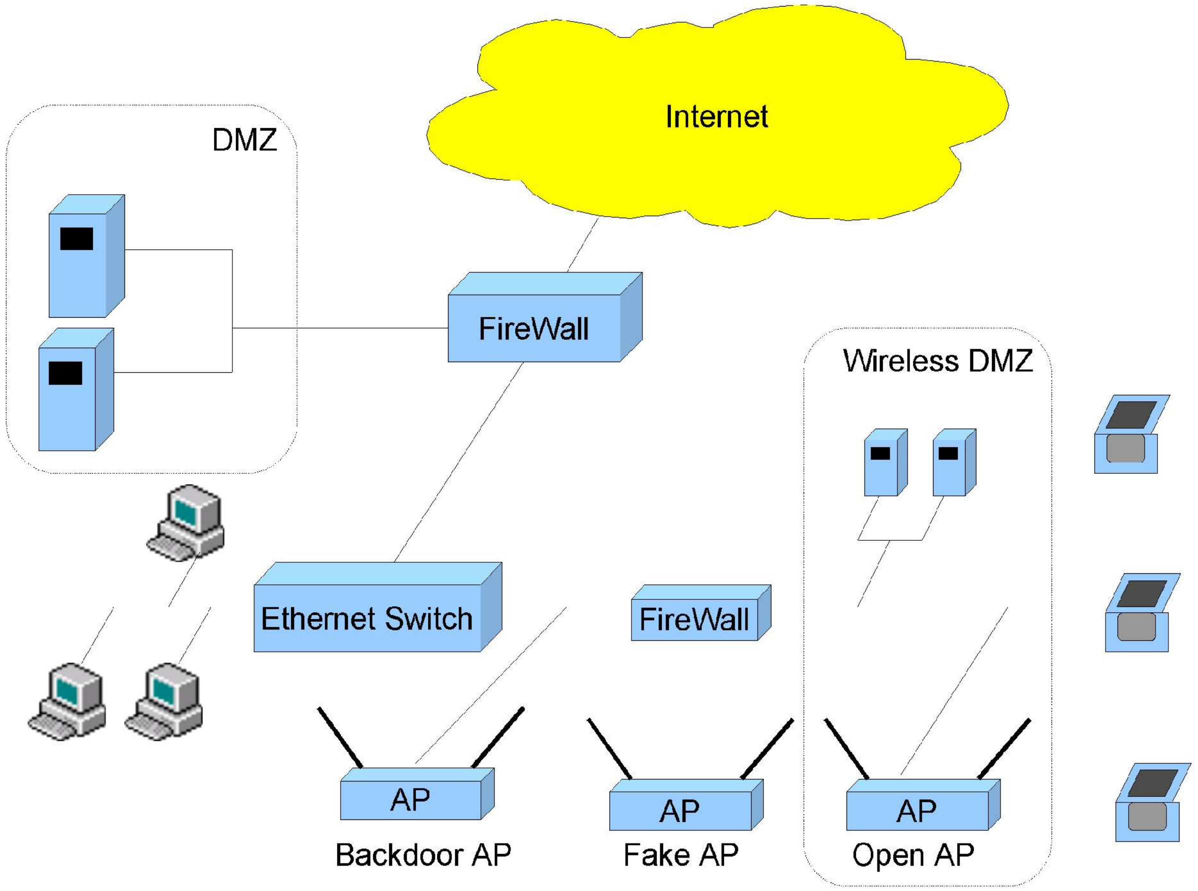

Figure 2: Backdoor Access point, Open Access point, Fake Access point in network topology

Fake access points are usually setup by intruders to mislead the authorized users (similar to a honeypot approach) and to capture their identification information or to perpetrate a man-in-the middle attack. Malicious fake access points usually will have the same SSID as the organization's managed access points, but can also have a similar looking SSID to make detection more difficult. Although the organization itself may also sometimes be tempted to set up a fake access point to attract potential attackers (Valli,C. 2004), non-malicious fake access points are not covered in this paper. As discussed in the previous section, implementing the correct mutual authentication on the wireless network may prevent the use of fake access points in attacks on the encryption protocols, but the detection of fake access points should in our view have a high priority as well, as they may indicate the existence of an implementation weakness in the organization's network architecture or the existence of a new, still unknown, man-in-the-middle attack (Figure 3) on the corporate network.

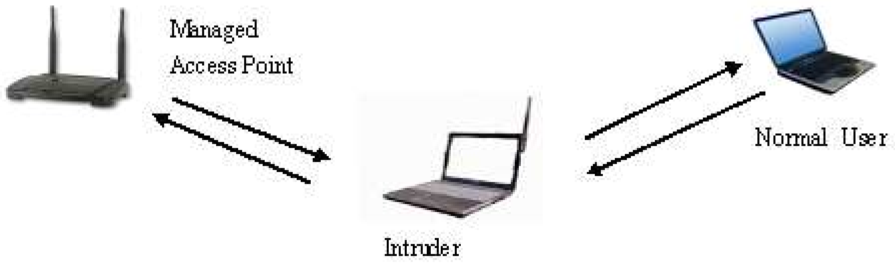

Figure 3: Man-In-the-Middle Attacks

The following table lists the difference between backdoor access points, open access points and malicious fake access points.

Table 1. Summary of difference between Backdoor access points, Open access points and Malicious Fake access points

Backdoor Access Points	Open Access Points	Fake Access Points
Physically located inside the organization's buildings in most cases;	Physically located inside the organization's buildings;	Physically locate either inside or outside the organization's buildings
Connected to the organization's wired network;	Connected to the organization's Wireless Demilitarized Zone;	- Malicious AP outside building will not have direct access to the organization's wireless network; - Malicious AP inside building might be connected to the organization's wireless network;
Have incomplete or none of security setting enabled;	Have incomplete or none of security setting enabled;	May have similar security settings as the organization's managed AP, making it more difficult to discover;
Operating channel can be any possible channel;	Operating channel can be any possible channel;	Using the same operating channel as managed APs would make malicious APs more difficult to be discovered and distinguished;
May change MAC to the same MAC address of another remote managed access point to avoid detection;	MAC address unchanged;	May change MAC to the same MAC address of another managed access point to avoid detection;
Any SSID name is possible	Uses the original SSID of the network	Same or similar to SSID used by managed AP

CURRENT STATE-OF-THE-ART IN AP DETECTION

There are currently a number of Intrusion Prevention Systems on the market capable of detecting incorrectly configured managed AP, intruder, normal user and managed access points and some other rogue access point. While, these intrusion prevention systems may also have some other limited intrusion detection capabilities, they seem to be mostly describing themselves as tools that can be used to ensure that the security configuration is correctly implemented in every access point.

Patrol Approach

In the patrol approach, an organization uses the same method as an attacker to discover the existence of access points. While it is possible to also use the same software as an attacker, some vendors of wireless intrusion prevention systems provide their own software and hardware to detect rogue access points; for example, Laptop Analyzer and Handheld Analyzer from AirMagnet (Airmagnet 2005).

Although this approach can be very effective to discover all kind of access points, it is also very time consuming and error prone. A good example is Netstumbler (MiniStumbler for PDA) (Netstumbler 2005). It has excellent usability design and support a broad range of wireless cards. By holding a laptop or PDA which is running Netstumbler and patrolling all the organization's buildings, information about access points can be built such as, whether they have any security configuration enabled and what kinds of security setting. However, it is more difficult to figure out the exact location of those access points, and to distinguish between a rogue access point and a legitimate access point from a nearby neighbor.

As it is also very time-consuming to patrol, especially in a large organization, it will be too expensive for most organizations to patrol frequently. Hence, the patrol approach will only give a snapshot of current wireless networks, and will be most effective against non-malicious rogue access points. People who intentionally set up a backdoor access point, however, might be trying to avoid detection by network administrators. As stumbler-like software often keeps sending Bacon frame to actively search access points, skillful intruders would be able to detect the patrol (Wright, J., 2002) and hide for a while.

RF surveillance Approach

Another popular approach is to place fixed sensors in the organization to continuously monitor the network and report to a central intrusion prevention server. Sensors work on Radio Frequency Monitor (RFMON) mode and are able to capture most of traffic frames within it reachable range. AirDefense Enterprise (Airdefense 2005), AirMagnet Enterprise (Airmagnet 2005), and research from (Lim,Y.X., Schmoyer,T., Levine,J. and Owen,H.L., 2003) are based on RF surveillance approach.

By monitoring the frame exchange between clients and access points, sensors will be able to discover the existence of any active access points. It seems straightforward that more sensors will mean a better coverage (more cells) and detection that is more accurate (less switching between the many possible frequency bands). Unfortunately, more sensors will also increase the cost of these systems.

Although the intrusion prevention server will combine all the information from different sensors and generate a complete picture of organization's wireless networks, it may again be difficult to distinguish legitimate access points from another organization from backdoor access points in their own organization. It will also be difficult to distinguish fake access points that use a legitimate but fake MAC address from the real access point.

The RF Surveillance Approach is excellent solution to detect any changes in the organization's wireless network in that it can offer 24x7 monitoring. This makes it appropriate to detect the insertion of a new access point, but may need to be combined with the patrol approach to decide whether the new access point is a fake access points or a backdoor access point.

Unfortunately, the RF surveillance approach does have several shortcomings as well. As mentioned earlier, this approach can be very costly. As the number of sensors increases there will be a larger expense for the dedicated wired networks between the sensors and the intrusion prevention server. Secondly, the effectiveness of this approach will depend largely on sensor placement. Due to the capacity of each sensor, it can be difficult to find the best position to place the sensor in a building (Yeo et al, 2004). It may therefore require a large amount of effort to design and fine-tune the deployment of sensors. Finally, the main challenge remains the collection and synchronization of a large volume of data from multiple sensors (Yeo et al, 2004).

Integrated approach

Some of vendors have integrated functionalities into their systems to detect illegal access points connected to an organization's wireless network. An example is the Wavelink Mobile Manager on Proxim ORiNOCO Access Points (Proxim Wireless Networks 2005).

In the integrated approach there is an extra component in the network architecture, called the Mobile Manager. The Mobile Manager generates a list of managed access points and a list of wireless clients connecting to an organization's networks. Continuously the Mobile Manager compares the list of all wireless clients found and its own list of all current wireless clients. If there is any mobile device connecting to the organization's network but not associating with any managed access points, this mobile device must have connected to a fake Access Point.

However, it is unclear whether this approach would be effective. As most characteristics on wireless devices are software changeable, it is possible for a skillful attacker to pretend to be the legitimized clients in order to avoid being detected.

Summary

The Patrol approach is most appropriate to detect the existence of open access points, especially for technical personnel to detect if they mis-configured any access points. By a careful assessment of each access point found, and trying to get an approximate location of the access point, a skillful user of the patrol approach may also be able to distinguish between a legitimate access point and a permanent backdoor or fake access point.

The RF surveillance approach and the integrated approach are appropriate to detect any changes in a wireless network. It makes RF surveillance approach more effective to detect malicious fake access points and Backdoor access points that are inserted after organization's wireless networks are completed.

CONCLUSION

While an enormous effort has been put into the design and implementation of wireless authentication to prevent any attacks that may weaken the encryption that is so crucial for wireless networks, it is unclear whether these new implementations of mutual authentication really have no weaknesses until a few years from now. We do know, however, that there are several ways in which these security measures can be circumvented and we have discussed our major concern, the danger presented by rogue access points, in this paper.

Open access points and non-malicious backdoor access points are like an unlocked door for any potential intruder. By utilizing Netstumbler or Kismet, attackers can easily discover these access points and utilize them from a large distance (Wiecking,B., 2002). While an intrusion prevention system can utilize the same tools to detect these access points, it is much more difficult for a defender to make sure that all of them are detected.

A malicious backdoor is the most dangerous rogue access point and, if it is configured to avoid detection, may only be detected while it is in use. Even then it may still be difficult to distinguish it from the many other legitimate access points visible in the same area. Malicious fake access points are traps set up by intruders. They intend to assign access points the same SSID as managed access points and might even have the similar authentication mechanism. When normal users connect to a fake access point the attacker can record their authentication information unless full mutual authentication is in place. More advanced attackers might use other Man-In-Middle attacks to hijack the session or to compromise one or both of the end-points.

Moreover, the defense against detected rogue access points is not straightforward. Although some research has proposed the use of Denial of Service attacks against intruders (Wright, J. 2005), we withhold our agreement on that. In our view, any active response to an intrusion would possible provoke intruders to launch more severe attacks. More importantly, the intruder can exploit this response and attempt to redirect the attack of the intrusion detection system to a legitimate wireless station by using its MAC address.

While attacks using these rogue access points are not the only attacks that can circumvent the Maginot line of wireless authentication, they are in the authors view the most urgent ones to address. This paper has argued that, while it is easy to detect potential access points, distinguishing between actual rogue access points and legitimate access points of their own organization and other organizations is a major problem. Solving this problem should be a priority for future research in wireless intrusion prevention systems.

REFFERENCE

Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J. & Levkowetz, Ed., (2004), Extensible Authentication Protocol (EAP), RFC 3748, June 2004

Airdefense (2005), http://www.airdefense.net/ (accessed 05/07/2005)

Airmagnet (2005), http://www.airmagnet.com/ (accessed 05/07/2005)

Baek,K.H., Smith,S.W. and Kotz,D., (2004), A Survey of WPA and 802.11i RSN Authentication Protocols", Dartmouth College Computer Science Technical Report TR2004-524, www.ists.dartmouth.edu/library/TR2004-524.pdf, (accessed 05/07/2005),

Bahl,P., Venkatachary,S. and Balachandran,A.,(2001) Secure Wireless Internet Access in Public Places, Communications, 2001. ICC 2001. IEEE International Conference on Volume 10, 11-14 June 2001 Page(s): 3271 – 3275 vol.10

Beyah,R., Kangude, S., Yu,G., Strickland,B. and Copeland,J., (2004), Rogue Access Point Detection using Temporal Traffic Characteristics, Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE Volume 4, 29 Nov.-3 Dec. 2004 Page(s):2271 - 2275 Vol.4

Cisco System Inc., (2002), Cisco Aironet Response to University of Maryland's Paper, 'An Initial Security Analysis of the IEEE 802.1x Standard', http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1680_pp.htm (accessed 05/07/2005)

IEEE Std 802.1X (2001), IEEE Standard for Local and metropolitan area networks—Port-Based Network Access Control _ IEEE Std 802.1X-2001

Intel (2005), Moore's Law, The Future, http://www.intel.com/technology/silicon/mooreslaw/ (accessed 05/07/2005)

Lim,Y.X., Schmoyer,T., Levine,J. and Owen,H.L., (2003) Wireless Intrusion Detection and Response, Proceedings of the 2003 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY, June 2003, pp68-75

Luo,H. and Henry,P.(2003), A Secure Public Wireless LAN Access Technique That Supports Walk-Up Users, GLOBECOM 2003, pp 1415- 1419

Mishra,A. and Arbaugh,W.A, (2002), An Initial Security Analysis of the IEEE 802.1X standard", CS-TR-4328, http://www.cs.umd.edu/~waa/1x.pdf (05/07/2005)

Netstumbler (2005), http://www.netstumbler.com/, (accessed 05/07/2005)

Phifer, L., (2003, "802.1x port access control for WLANs", http://www.wi-fiplanet.com/tutorials/article.php/3073201 (accessed 20/08/2005)

Proxim Wireless Networks (2005), White Paper, "Rogue Access Point Detection: Automatically Detect and

Manage Wireless Threats to Your Network"

Schmoyer,T.R., Lim, Y.X.,and Owen,H.L., (2004) Wireless intrusion detection and response: a classic study using main-in-the-middle attack, Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE Volume2, 21-25 March 2004 Page(s):883 - 888 Vol.2

Valli,C. (2004), Wireless Snort – A WIDS in progress, FORENSICS 2004, Perth, Western Australia, November 24-25, 2004

Webb, S (2003), Identifying trends in 802.11b networks in Perth, the Australian Computer Network, Information & Forensics Conference, Perth, 2003

Wiecking,B.,(2002), Maui High Performance Computing Center, "Wireless Security Overview"

Wong,S.,(2003), The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards, SANS Institute 2003

Wright, J., (2002) Layer 2 Analysis of WLAN Discovery Application for Intrusion Detection, http://home.jwu.edu/jwright/ (accessed 05/07/2005)

Wright,J., (2005), "Weaknesses in Wireless LAN Session Containment", http://i.cmpnet.com/nc/1612/graphics/SessionContainment_file.pdf (accessed 20/08/2005)

Yek, S. and Bolan, C. (2004), An analysis of security in 802.11b and 802.11g wireless networks in Perth,W.A., The 2nd Australian Information Security Management Conference 2004 (InfoSec2004), Perth, Western Australia, November 24-25, 2004

Yeo,J., Youssef,M. and Agrawala,A., (2004),A Framework for Wireless LAN Monitoring and Its Applications, WiSe'04, October 1, 2004, Philadelphia, Pennsylvania, USA, pp70-79

COPYRIGHT