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.

The Limits on Wireless Security: 802.11 in early 2002

As argued here, wireless networks are inherently less secure than wired networks. However, that does not mean that they are too insecure to be usable. In the wireless world, the range goes from public community networks designed to be accessed by everybody to military networks where lives can be lost if they are compromised. The greater vulnerability of wireless networks does mean that their security problems should be regarded differently, as networks that require measures in addition to those taken for their wired co...

Copyright SANS Institute

Author Retains Full Rights

AD

The Limits on Wireless Security: 802.11 in early 2002

James Voorhees
Security Essentials GSEC Practical Assignment Version 1.3 (Amended December 12, 2001)

SUMMARY

The rapid growth and change of 802.11 technology means that the security problems of wireless networks is poorly understood. Yet wireless networks present problems for security not present in wired networks. As they connect through the air, which offers no easily delimited set of points to defend. The medium makes eavesdropping a threat, interference a problem, and the interception of transmissions easier than on wired networks. Encryption is essential. The mobility of the devices on a wireless network and the extension of the technology to many types of devices restricts the solutions that can be devised.

Both authentication and encryption are problems in the 802.11 standard. WEP is essential to both, but problems have been found in the ways it handles its initialization vector and keys. The location of wireless networks, both physical and logical is another important element in making these networks secure. The new standards now being used in products, 802.11a and 802.11g, are not likely to affect security much. Other standards may be different. 802.1x and the work of the 802.11g Task Group, on the other hand, are likely to provide measures that can increase the security of 802.11 networks.

Wireless networks are inherently less secure than wired networks and must be treated so. Yet if proper measures are taken, they can be made secure enough to meet the needs of most people and organizations.

INTRODUCTION

Wireless networks are proliferating as the cost of the technology has fallen and as new uses for them are found. Because they can be installed without the cost of laying cable, they are increasingly common in the home. They provide a cheaply, easy way for people to connect in public spaces, so they have proliferated in airports and coffee shops. Two conferences I attended last year made Internet access freely available through wireless LANs. Some people see them as publicly available alternatives to commercial broadband services (Flickenger). They are also proving their value in emergencies, where they can provide rapidly deployable access to computer resources. The installation of a wireless LAN at the Pentagon after the September 11 attack is a case in point. At a time when investment in information technology is falling, wireless networks are still growing: 3.3 million units were shipped in 2000; one estimate has more than seven times that many, 23.6 million will be shipped in 2005 (Cyberatlas 2001).

Not only is the technology becoming popular at an exponential rate, it is also changing rapidly. Much of what is available now is new and little tested by real-world experience. Moreover, the open standards that the technology uses are still being set—new ones almost seem to appear monthly, companies issue new products frequently, and proprietary solutions to the myriad problems of the technology are proliferating.

The rapid spread of the technology, its novelty to many, and the changes it is still undergoing mean that the limitations on operating a wireless LAN securely are poorly understood. Concerns about

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

security are mounting. Indeed, as the executive director of the Wireless LAN Association noted, "Security concerns have become the most visible challenge to Wireless LAN growth in the enterprise market" (Abramovitz 2001). Well-publicized flaws in the wireless encryption protocol (WEP) and the spread of "war-driving" might make it seem that wireless networks are best regarded simply as insecure networks.

The publicity about wireless LAN security, oddly enough, has not yet included exploits by the hacker community. War driving has been used largely to find networks, not to penetrate them (Ellison 2001; Keeney 2001; Poulsen 2001). So far. In the near future, however, expect to hear that wireless networks have been hacked, viruses have proliferated through such networks, and that other hacker exploits have wreaked havoc. These will strengthen the impression that wireless networks cannot be made secure and increase the need to ensure that they are as secure as they can be.

It is my contention, argued here, that wireless networks are inherently less secure than wired networks. However, with a proper understanding of the limits on the security of these networks, one's security needs, and what can be done to secure the information that flows over these networks, they can nonetheless continue to provide a valuable means of communication for the people and organizations that choose to deploy them.

While many of the issues discussed in this paper are important for home networks, its focus will be on organizational networks. It will focus on networks that use the 802.11 standard. Other standards are used, such as Bluetooth, HomeRF, and HiperLAN, but 802.11 is currently the most widespread protocol for wireless networks in the United States, and its popularity is driving the expansion of wireless LANs.

The Technology, Briefly

Wireless LANs use radio transmissions. This means that many of the security concerns peculiar to wireless LANS stem from qualities that should be recognizable to those familiar with radio in its many manifestations, such as AM-FM, short wave, police band, and citizens band. Yet many of these technologies are designed to reach as many people as possible, privacy is a secondary concern for the rest, and there are no "jewels" stored on any. Most wireless networks, in contrast are designed to connect a finite set of users who make transmissions that must be kept private. In addition, either the networks themselves of networks they are connected to have data stored whose loss, theft, or destruction would come at a significant cost.

The 802.11 standard is a networking technology that uses either a peer-to-peer or client-server model. The peers or the clients are called stations. They are connected using a client card with the necessary software. The client card includes a radio transceiver and participates actively in the process of associating with a network. Stations that connect directly with each other form an independent basic service set (IBSS), which operates in ad hoc mode. The "servers" (more like hubs, actually) that are used to connect stations are access points (APs), each one identified by a service set identifier (SSID). A network that connects stations through a single access point is a basic service sets (BSS). A network that connects stations through several access points is an extended service set (ESS). Both BSSs and ESSs operate in infrastructure mode.

802.11 networks spread their transmissions over a spectrum of frequencies, in contrast to AM, FM, or short-wave, which transmit over single frequencies. They can use either of two methods to do

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

this, frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS) transmissions. The 802.11b, 802.11a, and 802.11g standards allow only the use of DSSS transmissions (the 802.11 standard itself also allows FHSS transmissions).

The use of spread spectrum transmissions complicates the task of intercepting or interfering with a transmission. But with the widespread adoption of wireless LANS and dissemination of the specifications, this complication can be regarded as trivial in the current environment. Arguments have been made that either FHSS or DSSS are more secure than the other (Zyren, Godfrey, and Eaton 2001), but, given the current dominance of 802.11b in the market, any difference can be considered irrelevant for the purposes of this paper.

802.11 networks transmit over one of two industrial, scientific, and medical (ISM) bands. 802.11b networks work on the 2.4 GHz band. So do a variety of other devices. 802.11a networks run on higher frequencies, in the 5 GHz band. This makes the 802.11a standard incompatible with 802.11b. The emerging 802.11g standard will also run in the 2.4 GHz band.

The Problem

The medium of transmission for wireless networks is the air, not a wire. You can limit physical access to the latter, but not the former. Nor does the owner of the wireless network own the medium. For that matter, the wireless network may transmit beyond the area that the owner of the network controls. Access can be gained to a wired network only through the hardware of the network, which present a limited set of points to defend. With wireless networks, the medium itself provides the attacker with infinite places to attack. This can mean that a wireless network is vulnerable to eavesdropping from hundreds of yards away. Just as police radio transmissions can be heard by many people they are not intended for, so can the transmissions of wireless LANs. It is not enough to limit access to the network through authentication, by closing ports, by hiding users behind a firewall, or disconnecting the network from the Internet. The transmissions themselves must be made secure. This makes encryption essential and makes it easier to intercept the transmissions used for authentication.

The mobile nature of wireless communications means that devices will sometimes move between access points. This increases the authentication problem, particularly if users expect to be able roam between access points easily and seamlessly, without losing connectivity.

As they use radio transmissions, wireless LANs are vulnerable to interference. Unintentional interference must be taken into consideration in setting up a wireless LAN in the first place. After all, 802.11b networks use the same frequency as microwave ovens, photocopiers, cordless telephones, and other common devices. This will be less of a problem with 802.11a networks, which run on a different frequency. Intentional interference—jamming, or a denial of service attack—has not been an important problem as yet. But it should be taken into consideration by the military or other security forces that might need to use wireless LAN to make time-sensitive transmissions in a hostile environment (Nichols and Lekkas 2002; Feldman 1998).

In addition, wireless networks often include many types of stations (a station is an 802.11-compliant networked device (Geier 2002). Laptop computers are the devices attached most often, but mobile handheld devices such as scanners, personal digital assistants (PDAs) and small computers powered by the PalmOS and Windows CE are becoming more common as well. Many of these have severely limited resources that can limit the security tools available or constrain how they are used. They also

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

have different operating systems and different interfaces with access points, other devices, and software. This complicates the task of distributing code-based solutions to security problems.

CURRENT SOLUTIONS

As noted above, the 802.11b standard is currently dominant. This may change as devices with the 802.11a or 802.11g standards come onto the market, or as rival standards mature. It has been recognized that the standards by themselves provide only the beginning of security. Even when the secure options are chosen, such as activating WEP, they must be supplemented by other means.

Authentication

Every station on a wireless LAN must be authenticated before it can associate with the network. There are two ways of authenticating, Open System and Shared Key. Both methods authenticate machines rather than users, which can make it difficult to track unusual activity and can add to the danger posed by the compromise of a machine. They also authenticate the station to the access point, but not the access point to the client, which opens the threat that a rogue access point will be inserted.

The Open System method is the default authentication algorithm, according to the 802.11 specification. It was designed primarily to facilitate access; it provides little security. The station that wants to associate with the network sends a frame identifying itself and asks for authentication. The access point (or other station) responds affirmatively. The entire process is done in clear text, without encryption.

Shared key authentication can only be adopted if Wired Equivalent Privacy (WEP) is enabled. The process of authentication begins the same way, with a frame sent to the authenticating station or access point. The response, however, and the rest of the dialogue uses text with a shared key. As with WEP encryption in general, the weakness here can be the key itself (Weatherspoon 2000).

Other means of authentication can be used to make authentication more secure. The authentication mechanism provided by the operating system is one. RADIUS and Kerberos (used in Windows 2000 networks) are two of the most common. These too have their problems (Hill 2001; Aboba and Palekar 2001;Wu 1998), and both rely on the strength of the passwords chosen. If the passwords are weak, so will be the security they provide. RADIUS, Kerberos, and other alternatives also add to the cost and complexity of a wireless network. An increase in cost or complexity may not be an insignificant consideration for a technology that is becoming popular because of its low cost and convenience. These other means can, nonetheless, do much to make authentication secure, particularly if the vendor and the administrator choose secure methods of implementing the standard, such as a credible random number generator for the request authenticator in RADIUS and requiring users to select strong passwords. In addition, the emerging 802.1x standard is designed to increase the security of authentication by centralizing it.

Encryption

The 802.11 standard includes WEP, which uses the RC4 stream cipher to encrypt the message. WEP is not enabled in most implementations. It does not encrypt an entire transmission, but only the data packets. Nor does not protect the physical layer header that includes control information for

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

managing the network (Geier 2002). That is not critical. But a copy of the initialization vector (IV), which is an essential part of WEP encryption, is also sent in the clear.

It is widely recognized that the protocol itself is flawed. It is being improved and may be replaced as a result of the deliberations of the 802.11i Task Group (Walker 2001). As it stands now, however, WEP will protect against the casual attacker—something is better than nothing—but it will not be proof against an attacker with a little determination, a few resources, and access to tools such as WEPCrack and Airsnort.

Briefly, WEP takes the message to be transmitted and appends a 32-bit cyclic redundancy check to create the plaintext. A 24-bit initialization vector (IV) is appended to a 40-bit or 104-bit key. The two together are transformed into a pseudorandom key stream using the RC4 algorithm. The plaintext and the key stream are then exclusive-ored (XORd) bitwise to generate the ciphertext, which is then transmitted to the recipient. Decryption simply reverses the process (Borisov et al. 2001).

Each element in the key stream is an essential weakness in the protocol. The issues surrounding the IV and the keys will be discussed separately below. The encryption algorithm (RC4) itself is also a problem.

While RC4 may be useful elsewhere, it has weaknesses as it is used in WEP, weaknesses related to the way WEP handles keys (Fluhrer, Mantin, and Shamir, 2001; Stubblefield, Ionnadis, and Rubin 2001; Walker 2000). Even the creator of RC4 finds that RC4 is unsuited to WEP (Rivest 2002). Fixes are being devised to WEP, notably fast-packet keying described below, that should solve most problems currently recognized. But until another algorithm replaces it, an essential weakness in WEP will remain.

The Insecurity of the IV

There are two problems with the IV in WEP. First, it is sent in the clear with the encrypted part of the packet. It is sent unencrypted so that the receiving station can use it in decryption. Second, the number of values the IV can take is limited to 2^{24}. Neither characteristic of WEP would be a problem if WEP were designed differently. What makes them both a problem is that a repeated combination of IV and key can ease an attacker's access to the plaintext: if two ciphertexts are XORd, the key stream cancels out, leaving the XOR of the plaintexts (Borisov, Goldberg, and Wagner 2001; Walker 2000).

In WEP, the IV varies with each packet. In the original 802.11 specification, the key remained constant. This combination was intended to ensure that the key stream of each packet was different. However, unless the key itself changes before the IV repeats, the key stream will repeat. But a busy access point can run through 2^{24} IVs in a matter of hours (Borisov, Goldberg, and Wagner 2001). And the birthday paradox, which is that in a room filled with as few as 23 people, the chances of two people having the same birthday are about 50 percent makes repetition likely to occur much more quickly. By one estimate, the probability that an IV will be repeated reaches near certainty—99 percent—after only 3 seconds of normal traffic (Walker 2000).

This assumes that the IV is changed after each packet. But this is not mandated by the 802.11 standard and is by no means a given with current implementations. Moreover, many cards on

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

laptops begin again at zero then begin to increment by one after they reinitialize, which they can usually be expected to do at least once a day.

The Insecurity of Keys

Like any symmetric key algorithm, knowledge of the key in WEP provides access to all messages (Schneier 1996). There is nothing in the 802.11 standard that defines how to distribute and manage keys. Yet security depends on the keys being kept out of the hands of would-be attackers. There are four questions in regard to keys that an implementation of a wireless network must answer: How is a key formed? How are keys distributed? How many keys are available? How often are they changed? The IEEE is standard is silent on many of these issues, which must be addressed when implementing a LAN. This means that some of the answers to these questions can only be found in proprietary solutions.

The 802.11 standard provides for two methods of producing keys (Arbaugh, Shanker, and Wan 2001). One is to create four default keys manually. These can be 40-bit keys, according to the standard. In many implementations now, the keys can be 104 bits long (this plus the 24 bit IV produce the 128 bit encryption that is often advertised). Though longer than a typical password, these keys suffer from the same malady: ill-formed, they can become vulnerable to dictionary attacks (CISCO 2001) or even clever guessing.

The other method, not yet widely supported, maps a key to a MAC address (Borisov, Goldberg, and Wagner 2001. The value of a key need not resemble the address; but each address should have its own key. The mappings table should have at least ten entries. There is no clear maximum other than the ability of an administrator to manage them. That can be a significant constraint as it can mean a trade-off between the size of a network and its security. As with much of key management, a proprietary solution can fill this gap.

Another gap is in how the keys are distributed. The standard merely assumes that a secure method of distribution is used. Again, a proprietary solution can help. The method of distribution also affects how often keys are changed. If they are changed manually, as is sometimes the case, it is likely that stations will have their keys changed but rarely. Particularly as wireless networks grow large, it becomes important that the distribution of keys become painless for the administrator.

There are other weaknesses in the way the 802.11 manages keys. The two methods of developing keys produce device-based, not user-based keys. This is a weakness because, after all, machines don't hack, people do; authenticating devices rather than users creates a security hole that can allow an attacker working on an authenticated device get access to a network. Moreover, as a shared-key encryption method, the security of the stations on which the keys are stored becomes important; a lost key can fall into the wrong hands. Another possible weakness is when the same key is used for both authentication and encryption—this increases further the possibility that a key stream will repeat.

The 802.11i Task Group recently approved a fix to the key and IV problems with WEP (Sayer 2001) that should find its way into 802.11 implementations soon. The fix assumes that 128-bit encryption is used. It works in two phases. The first phase mixes a 128-bit secret key with the MAC address of the transmitting device. This can be cached and reused. The second phase combines the output of

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

the first with the IV. The result is an RC4-encrypted key stream that will be different for both the transmitting device and the receiving device (RSA Security 2001; Housley and Whiting 2001).

Security by Location

Wireless LANs need to be developed with location in mind. The physical location of access points determines how well users can be connected. The points must be placed so that users can connect, yet away from sources of interference such as microwave ovens and Bluetooth devices. Both the physical location and the logical location have implications for security that must be considered when the network is being designed and set up.

Physical Location

The physical security of the both stations and access points are important for network security. Some of the reasons for this were pointed out above. Stations, usually mobile devices such as laptop computers, are vulnerable for much the same reason as similar devices that run on wired networks. For wireless networks, not only is the security of the data on the machine at risk if a machine is lost or "borrowed," but, as noted before, the key used in WEP encryption might be stolen, especially in static-key implementations. An access point should be located so that it cannot be tampered with. This could be high on a wall or in a wiring closet.

To minimize the potential for eavesdropping, access points should be placed to minimize the distance that the signal can travel outside the area under the control of the organization (Blackwell 2002). This might be close to the center of the building. For the same reason, the gain on the access point should be reduced to the minimum necessary to connect the users. This follows the principle that a network should provide the least access those who use it require. It will reduce the threat of eavesdropping. It cannot end it, however, particularly given that directional antennas greatly increase the distance from which an eavesdropper can "hear" the transmissions." One reporter, working in Manhattan, was able to identify networks in buildings six blocks away (Ellison 2001).

Logical Location

Wireless networks should be treated as insecure counterparts to their wired associates, with restricted access to resources on the wired network. They should, therefore, be kept separate, with the "crown jewels" of an organization kept, one might say, tethered. A firewall between the wired and wireless networks will increase security significantly. One recommended step is to establish rules that allow only machines with the IP or MAC addresses of recognized users access through the firewall to the wired network (Blackwell 2002). A firewall, however, can actually reduce security if they are regarded as a panacea, as a solution to all the security problems of wireless networks in itself. Instead, it must be seen as but one part of a layered approach to security.

Much the same can be said of VPNs. They can provide a useful but incomplete solution to security problems. Moreover, they can be expensive and add to the complexity of a network. The expense can make them unsuitable for smaller networks (Convery and Miller 2001).

THE FUTURE

Wireless security is a moving target. New standards are still being approved by the IEEE. New products based on those standards follow months of that approval. In addition, proprietary-based

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

solutions to security problems that attempt to fill the lacunae left in the standards are appearing constantly. The technology for wireless LANs is far from mature.

New Standards

Several new standards have been approved and are beginning to appear in commercial applications. These include 802.11a and 802.11g. The security issues surrounding both are likely to be virtually the same as those that surround 802.11b networks. The latter, just approved, will provide faster speeds on the same frequency as 802.11b. The former will run in a different frequency band. Networks that follow the 802.11a standard are less likely to suffer interference, intentional and otherwise, than 802.11b networks. They will have a lower range, which should, at least initially, make it somewhat more difficult to eavesdrop. As time goes on, however, and both attackers and defenders gain experience, any differences in the security of these networks that use these standards and 802.11b networks are likely to disappear.

In addition to the work being done in the IEEE to create new standards for wireless LAN transmission, the 802.11i Task Group has been created to develop standards that will increase the security of 802.11 networks. It is now working on ways to fix WEP, but it can be expected to develop a replacement in which the Advanced Encryption Standard (AES) replaces RC4 (Walker 2001)

One of the standards now emerging is 802.1x, originally designed for wired Ethernet networks. It provides a centralized, port-based framework for authentication that relies on the PPP Extensible Authentication Protocol (EAP) and allows use of an authentication server (Roshan 2001; CISCO 2001; Blunk and Vollbrecht 1998). This server does not have to be a RADIUS server, but it often is. A port in this context is simply a point at which a device is attached to a LAN.

The 802.1x standard has not yet been approved, but implementations have already been put on the market by CISCO, Microsoft, and several other firms. A problem with the standard as it is emerging is that while it makes possible a significant improvement in authentication, it provides for no standard method that will be used throughout the authentication process. Indeed, both CISCO and Microsoft have adopted different schemes—CISCO has its Light EAP (LEAP) and Microsoft has included EAP-TLS in Windows 2000 and XP (CISCO 2001; Ayyagari and Fout 2001)—and other firms are finding their own schemes. This can only reduce the interoperability of 802.11 equipment and reduces the security of networks that use equipment from more than one vendor.

New Problems

As wireless LANS based on the 802.11 standard gain acceptance and the technology matures, the functionality of WLAN devices will increase. So will the range of devices that can be used on wireless LANs and the range of applications available. In particular, we can expect voice over IP to be run across a wireless LAN infrastructure (Abramovitz 2001). This will, at the very least, complicate the task of securing wireless networks.

In the more distant future, there are indications that wireless LAN technology will develop rapidly enough that the current standards will become obsolete much more quickly than, say, Ethernet. Wireless technology that make it possible to create networks that run in different frequency bands at

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

speeds of more than a gigabyte per second are more than a pipe dream (ComputerWire 2002). The security problems they pose may seem achingly familiar; but they may pose new challenges as well.

CONCLUSION

As argued here, wireless networks are inherently less secure than wired networks. That does not mean that they are too insecure to be usable. After all, there is no such thing as a perfectly secure network of any kind. Nor do all networks require the same amount of security. In the wireless world, the range goes from public community networks designed to be accessed by everybody to military networks where lives can be lost if they are compromised. The greater vulnerability of wireless networks does mean that their security problems should be regarded differently, as networks that require measures in addition to the measures taken for their wired counterparts. Indeed, many observers advise leaving a wireless LAN outside a wired network's firewall or through a VPN, treating wireless users much like remote users who connect through the insecure cloud that is the Internet.

Security for wireless networks, like that of wired networks, should be designed in layers. Indeed, many of the solutions that are advisable for wired networks should be applied to wireless networks as well. These include auditing systems, monitoring logs, using tools such as IDSs and sniffers, and enforcing strong passwords. Recommendations about how to increase the security of wireless networks can be easily found. They include the lists found in Blackwell 2002, Ellison 2001, Mahan 2001, Wireless Ethernet Compatibility Alliance 2001, and WLANA 2001. With proper security measures applied, wireless networks can be made secure enough to meet the needs of most people and organizations.

REFERENCES

Aboba, Bernard, and Palakar, Ashwin, "IEEE 802.1x and RADIUS Security." Doc.: IEEE 802.11-01/TBD.

Abramowitz, Jeff. 2001. "Wireless LANS—Poised for Untethered Growth." URL: http://www.wlana.org/pdf/wlana_industry.pdf.

Ayyagari, Arun, and Fout, Tom. 2001. "Making IEEE 802.11 Networks Enterprise Ready." URL: http://www.microsoft.com/windows2000/techinfo/administration/security/wirelessec.asp.

Alexander, Bruce and Henderson, Byron. 2001. "Wireless Networking Standards and Security Update." Networking Professionals Online Tech Talk, Cisco Systems. URL: http://www.cisco.com/go/ciscowebseminars/wireless2/L802-166-XA.

ANSI/IEEE Std 802.11, 1999 edition. *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.*

Arbaugh, William A.; Shankar, Narendar; and Wan, Y.C. Justin. 2001. "Your 802.11 Wireless Network has No Clothes." URL: http://www.cs.umd.edu/~waa/wireless.pdf.

Blackwell, Gerry. 2002. "Serious WLAN Security Threats: Part 1 and Part II." URLs: http://www.80211-planet.com/columns/article/0,4000,1781_949891,00.html; http://www.80211-planet.com/columns/article/0,,1781_947571,00.html.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Blunk, L. and Vollbrecht, J. 1998. "PPP Extensible Authentication Protocol (EAP)." URL: http://www.interlinknetworks.com/references/technical_materials/docs/rfc2284.txt.

Borisov, Nikita; Goldberg, Ian; and Wagner, David. 2001 "Intercepting Mobile Communications: The Insecurity of 802.11." URL: http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf.

CISCO Systems. 2001. "CISCO—Security for the Next Generation Wireless LANs." URL: http://www.cisco.com/warp/public/102/wlan/nextgen.html.

ComputerWire. 2002. "NTT Researchers Predict 10Gbps Wireless." January 24. URL: http://www.theregister.co.uk/content/5/23809.html.

Convery, Sean, and Miller, Darrin. 2001. "SAFE: Wireless LAN Security in Depth." URL: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm.

Ellison, Craig. 2001. "Exploiting and Protecting 802.11b Wireless Networks." URL: http://www.extremetech.com/article/0,3396,s%253D1024%2526a%253D13880,%2000.asp.

Feldman, Philip M. 1998. *Emerging Commercial Mobile Wireless Technology and Standards: Suitable for the Army?* MR-960-A. Santa Monica, CA: RAND. URL: http://www.rand.org/publications/MR/MR960/.

Flickenger, Rob. 2002. *Building Wireless Community Networks.* Sebastopol, CA: O'Reilly & Associates.

Fluhrer, Scott; Mantin, Itsik; and Shamir, Adi. 2001. "Weaknesses in the Key Scheduling Algorithm of RC4." URL: http://www.cryptonomicon.net/papers/rc4_ksaproc.pdf.

Geier, Jim. 2002. *Wireless LANS,* Second Edition. Indianapolis, IN: SAMS.

Hill, Joshua. 2001. "An Analysis of the RADUIS Authentication Protocol." URL: http://www.untruth.org/~josh/security/radius/radius-auth.html

Housley, Russ, and Whiting, Doug. 2001. "Temporal Key Hash." Doc.: IEEE 802.11-01/550r2.

Keeney, Frank. 2001. "Vacation War Driving from Pasadena, CA to San Francisco, CA." URL: http://www.pasadena.net/vacation.

Mahan, Robert E. "Security in Wireless Networks." November 14. URL: http://rr.sans.org/wireless/wireless_net3.php.

Nichols, Randall K., and Lekkas, Panos C. 2002. *Wireless Security: Models, Threats, and Solutions.* New York: McGraw-Hill.

Poulsen, Kevin. 2001. "War Driving by the Bay: Wireless Network Hacking Turns Cyber Attack into Street Crime," April 12. URL: http://www.securityfocus.com/news/192.

Rivest, Ron. 2002. "RSA Security Response to Weaknesses in Key Scheduling Algorithm of RC4." URL: http://www.rsasecurity.com/rsalabs/technotes/wep.html.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Roshan, Pejman. 2001. "802.1x Authenticates 802.11 Wireless." *Network World Fusion*. URL: http://www.nwfusion.com/news/tech/2001/0924tech.html.

RSA Security. 2001. "WEP Fix Using RC4 Fast Packet Keying." URL: http://www.rsasecurity.com/rsalabs/technotes/wep-fix.html.

Sayer, Peter. 2001. "Wireless LAN Security Fix on Tap from IEEE Group." January 7. URL: http://www.nwfusion.com/news/2002/128615_01-07-2002.html.

Schneier, Bruce. 1996. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Second Edition. New York: John Wiley & Sons, Inc.

Stubblefield, Adam; Ionnadis, John; and Rubin, Aviel D. 2001. "Using the Fluhrer, Martin, and Shamir Attack to Break WEP, Revision 2." August 21. URL: http://www.sublimation.org/security/localarchive/802.11/wep_attack.pdf.

Trudeau, Pierre. 2001. "Building Secure Wireless Local Area Networks." URL: http://www.colubris.com/en/support/whitepapers/whitepapers/WP-010712-EN-01-00.pdf.

Vollbrecht, John; Rago, David; and Moskowitx, Robert. 2001. "Wireless LAN Access Control and Authentication." URL: http://www.interlinknetworks.com/references/WLAN_Access_Control.html.

Walker, Jesse. 2001. "Tentative Minutes of TGi for Austin November 2001." Doc.: IEEE 802.11-01/348r0.

_____ . 2000. "Unsafe at Any Key Size; Analysis of the WEP Encapsulation." Doc.: IEEE 802.11-00/362.

Weatherspoon, Sultan. 2000. 'Overview of 802.11b Security." *Intel Technology Journal* (Quarter 2). URL: http://developer.intel.com/technology/itj/q22000/pdf/art_5.pdf.

Wireless Ethernet Compatibility Alliance. 2001. "WEP Security Statement." September 7. URL: http://www.wirelessethernet.org/pdf/20011015_WEP_Security.pdf.

WLANA. 2001. "WLANA Security White Paper." URL: http://www.enterasys.com/roamabout/WLANAsecwp.htm.

Wu, Thomas. 1998. "A Real World Analysis of Kerberos Password Security." URL: http://theory.stanford.edu/~tjw/krbpass.html.

Zyren, Jim; Godfrey, Tim; and Eaton, Dennis. 2001. "Does Frequency Hopping Enhance Security?" URL: http://www.wirelessethernet.org/pdf/20010419_frequencyHopping.pdf.

© SANS Institute 2002, 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