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.

Security in Wireless Networks

The 802.11 specifications include services for link-level authentication and an optional privacy (i.e., confidentiality) service termed Wired Equivalent Privacy (WEP). WEP is designed to protect the confidentiality of link layer traffic (i.e., the wireless leg). The security parts of the standard provide no claims about secure integrity assurance, but it does require a frame check sequence (FCS) error control mechanism. Research reports and press accounts have reported serious flaws in the authentication service and th...

Copyright SANS Institute
Author Retains Full Rights

AD

Security in Wireless Networks
Robert E. Mahan
November 14, 2001

Level One Security Essentials
Practical Assignment
Version 1.2f

Introduction

Local Area Network (LAN) standards are developed by the Institute of Electrical and Electronic Engineers (IEEE) 802 LAN/MAN Standards Committee. Some of the most widely used standards developed by IEEE are for the wired Ethernet family; Token Ring, Wireless LAN, and Bridging and Virtual Bridged LANs. A different IEEE Working Group provides the focus for each area.

The IEEE 802.11 standard specifies the requirements for implementing wireless Local Area Networks [LAN99]. There are two approved IEEE 802.11 specifications and two more are being developed [COX01]. IEEE 802.11 was ratified in 1997 and supports a data rate of 2 Mbits/second. It is not widely implemented because of its low speed and the availability of a faster alternative. IEEE 802.11b specifies rates up to 11 Mbits/second, was ratified in 1999, is supported by multiple vendors, and is widely accepted in the marketplace. IEEE 802.11g is under development and will support data rates up to 22 Mbits/second. Equipment is expected to be available in 2002. IEEE 802.11a is under development, operates at data rates up to 54 Mbits/second and is the emerging high-speed option. Equipment is expected to be available in late 2001 or early 2002.

The 802.11 specifications include services for link-level authentication and an optional privacy (i.e., confidentiality) service termed Wired Equivalent Privacy (WEP). WEP is designed to protect the confidentiality of link layer traffic (i.e., the wireless leg). The security parts of the standard provide no claims about secure integrity assurance, but it does require a frame check sequence (FCS) error control mechanism.

Research reports and press accounts have reported serious flaws in the authentication service and the WEP algorithm [BORI01][ARBA01][STUB01][WALK00]. We examine the technology in light of these claims and assess the security of the proposed implementation of wireless LANs.

Security Threats

All computer systems and communications channels face security threats that can compromise systems, the services provided by the systems, and/or the data stored on or transmitted between systems. The most common threats are:

- Denial-of-service

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Interception
- Manipulation
- Masquerading
- Repudiation

Denial-Of-Service (DOS) occurs when an adversary causes a system or a network to become unavailable to legitimate users or causes services to be interrupted or delayed. Consequences can range from a measurable reduction in performance to the complete failure of the system. A wireless example would be using an external signal to jam the wireless channel. There is little that can be done to keep a serious adversary from mounting a denial of service attack.

Interception has more than one meaning. A user's identity can be intercepted leading to a later instance of masquerading as a legitimate user or a data stream can be intercepted and decrypted for the purpose of disclosing otherwise private information. In either case, the adversary is attacking the confidentiality or privacy of the information that is intercepted. An example would be eavesdropping and capturing the wireless interchanges between a wireless device and the network access point. Since wireless systems use the radio band for transmission, all transmissions can be readily intercepted. Therefore, some form of strong authentication and encryption is necessary in order to keep the contents of intercepted signals from being disclosed.

Manipulation means that data has been inserted, deleted, or otherwise modified on a system or during transmission. This is an attack on the integrity of either the data transmission or on the data stored on a system. An example would be the insertion of a Trojan program or virus on a user device or into the network. Protection of access to the network and its attached systems is one means of avoiding manipulation.

Masquerading refers to the act of an adversary posing as a legitimate user in order to gain access to a wireless network or a system served by the network. For example, a user with inappropriate access to a valid network authenticator could access the network and perform unacceptable functions (e.g., break into a server and plant malicious code, etc.). Strong authentication is required to avoid masquerade attacks.

Repudiation is when a user denies having performed an action on the network. Users might deny having sent a particular message or deny accessing the network and performing some action. Strong authentication of users, integrity assurance methods, and digital signatures can minimize the possibility of repudiation.

Security Services and Vulnerabilities

Two security services are specified in IEEE 802.11, the authentication service and the privacy service. The privacy service is provided by Wired Equivalent Privacy (WEP) algorithm. The authentication service provides two basic levels of security. The first, Open System Authentication (OSA) is mandatory, but provides essentially no security.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The second is shared-key authentication that provides the highest level of security available and uses the WEP algorithm.

OSA exchanges messages between a station and the wireless access point. Any station that can successfully send and receive compliant messages is permitted to associate with and enter the network.

Shared key authentication specifies a number of requirements intended to defeat or mitigate some of the threats mentioned earlier. Particular attention was paid to 1) authenticating users over an encrypted channel, 2) defeating an adversary's ability to eavesdrop on wireless transmissions in order to preserve confidentiality by encrypting the channel traffic, and 3) providing integrity assurance that a message was not modified in transit.

Wired Equivalent Privacy (WEP)

The WEP is based on the use of RC4 encryption. RC4 is a stream cipher developed in 1987 by Ron Rivest at MIT for RSA data security. The algorithm was kept secret for the first 7 years, but was anonymously posted to the Cypherpunks mailing list in 1994 and it quickly spread to news and ftp sites around the world. Although it is now public, analysis indicates that RC4 is still a strong algorithm and is immune to linear and differential cryptanalysis, is very non-linear, and does not have short cycles. RC4 is used in many commercial products. RC4 as specified in the standard operates in Output FeedBack (OFB) mode as shown in Figure 1.

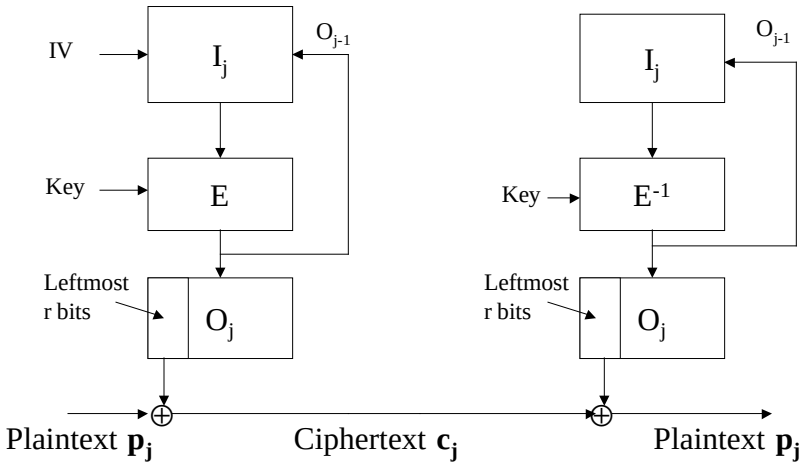

Figure 1. RC4 Operation.

The RC4 algorithm has three inputs; an initializing vector IV, the random key, and the plaintext. The IV vector is input to E, the RC4 encryption algorithm, along with the key. The algorithm generates a keystream output from E that is sent to the output box O. The output box O shifts the keystream out, a byte at a time and each byte is combined with the plaintext P under the Exclusive OR function. The output of E is also fed back to the I stage which causes the keystream to vary as a function of IV and the key.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

That is:

Given: The plaintext p_j and RC4(IV, Key)

Form: $c_j = p_j \oplus$ RC4(IV, Key)

Encryption is shown on the left and decryption on the right side of Figure 1.

Since IV must be known to the transmitter and receiver, it is sent to the receiver as an unencrypted part of the ciphertext stream. The logic function to insert IV into the ciphertext stream and recover it from the stream for input to the I function at the receiving end are not shown, but are straightforward functions. IV does not have to be secret since RC4's strength is derived from the algorithm and key, not IV. However, the integrity of IV needs to be assured or decryption will not function properly.

The RC4 algorithm supports variable length keys. The two lengths most commonly used for wireless applications are 40 bits for export controlled systems and 128 bits for domestic application. Although most vendors advertise 128 bit encryption, the effective key length is 104 bits [BORI01-1].

One of the primary requirements of stream ciphers in general and RC4 as well is that the implementation must ensure that the keystream is never used twice to encrypt a data stream.

Key Management

The standard does not specify how keys are managed or distributed. It does provide for an externally populated globally shared array of 4 keys. In addition, it allows for an additional array that associates a unique key with each user station. Most existing implementations utilize the globally shared array of secret keys to encrypt the link transmission between users and the wireless network access point. If a single key is used, it is made known to all users and the access point. If more than one key is used, it is known to all users in the group associated with the key. Some access points allow for two channels such that the keys for each channel can be different. Devices assigned to one channel still share the secret key with other users assigned to that channel and the access point.

Integrity Assurance

The plaintext input p_j string is composed of the original message M with a CRC32 checksum of the message appended to the end of the message. The purpose of the checksum is to provide the integrity service that is described later. Therefore:

Given: PM, a plaintext message string, compute the checksum of PM = c(PM) and concatenate the two parts to produce the plaintext P = PM, c(PM).

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

At the receiver the ciphertext is decrypted, the CRC32 bit string is calculated on the original plaintext input string and compared to the CRC32 received. If the CRCs match then the original message is accepted as valid. This is a well-known method for detecting the presence of errors in the received bit stream. The method does not ensure cryptographic integrity.

Vulnerabilities and Weaknesses

Authentication

Prior to sending data, a station (i.e., a wireless device) and an access point must authenticate and establish an association. An association is a binding between the station and the access point. The process for this consists of three states:

- Unauthenticated and unassociated
- Authenticated and unassociated
- Authenticated and associated

Once successfully authenticated and associated stations can exchange data with the access point (i.e., enter the network). As indicated earlier, two authentication methods are supported, Open System authentication and Shared key Authentication.

Open System Authentication

Open System Authentication (OSA) is a mandatory standard requirement and is the default authentication method. In OSA, two management frames are exchanged between the station and the access point (AP). The first frame is sent from the station to the AP and includes the station Media Access Control (MAC) address and an identifier indicating it is an authentication request. The AP responds with a second frame that includes a status field indicating authentication success or failure. The station is now authenticated and unassociated. Two more frames are passed to establish and association. Most wireless vendors have implemented a wireless access control mechanism as part of the association process that is based on examining the station MAC address and blocking unwanted stations from associating. Support for this requires that a list of authorized MAC addresses be loaded on each AP.

This approach has several problems. Identifying and loading MAC addresses and then keeping them current is manually intensive. An adversary seeking access to the network could monitor the network and capture legitimate MAC addresses, modify a station to use a permissible MAC address and associate with the AP gaining access to the network. This also has the potential to create network problems if two stations with the same address attempt to use the network at the same time.

In any case, OSA is not recommended. In the default case any requesting station can be authenticated and associated. In cases where the manufacturer of the network equipment

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

support MAC address access control, the addresses can be readily spoofed and allow inappropriate access as well as potentially causing network problems.

Shared Key Authentication

Shared key authentication uses the optional WEP algorithm along with a challenge response system to mutually authenticate a station and an AP. Authentication consists of the exchange of 4 messages for station authentication and 4 more for AP authentication.

APs send "beacon" messages to announce their presence. A station wishing to enter the network finds a beacon message and then initiates authentication with the AP whose address appears in the beacon message. The exchange is shown in Figure 2.

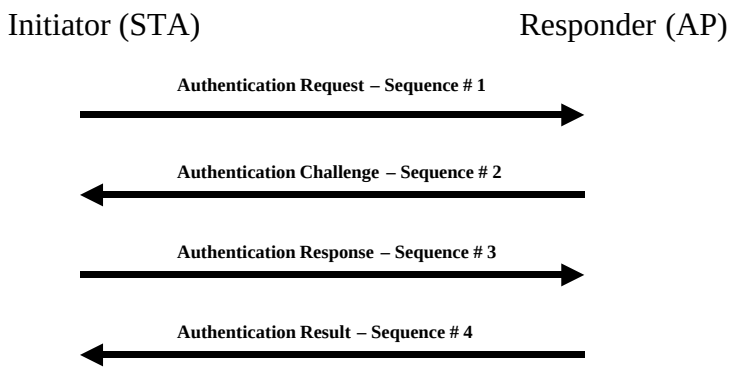

Figure 2. Shared key Authentication Exchange.

The initiating station sends a management frame (sequence # 1) to the AP requesting authentication. The frame is sent in the clear. The responding AP sends sequence #2 which contains an authentication challenge in the message body. The challenge is 128 octets in length.

The AP challenge is generated by combining a pseudo random number with the shared secret key and a random initializing vector (IV) and sent as a clear text message (i.e., unencrypted).

The station receives the message, extracts the challenge and copies it to a new management frame. This frame is encrypted under the WEP algorithm using the shared key and a "new" IV and sent to the AP. The IV used by the station is also sent to the AP in the clear so the AP knows what IV to use with the secret key to decrypt the frame.

The AP receives the frame, decrypts the contents, and checks the validity of the CRC 32 check sum, and tests the challenge to see if it matches the original challenge sent to the station. If the CRC 32 check is invalid, the frame is dropped. If the CRC-32 is valid, the challenge is tested. On a match, the station is successfully authenticated. The process is repeated to authenticate the AP to the station.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The protocol for exchanging authentication messages can be exploited to allow unauthorized stations to enter the network. In this exploit, an unauthorized station monitors the exchange just described and captures the second and third exchanges. The second frame contains the unencrypted challenge and the third frame contains the encrypted challenge. The unauthorized station has the following information:

- The plaintext of the original frame including the random challenge
- The encrypted frame containing the challenge, and
- The IV used to encrypt the challenge.

The exclusive OR of the plaintext P and the Ciphertext C will produce the keystream used to encrypt the challenge response frame. The unauthorized station will not have the shared secret key, but given the key stream, the unauthorized station can enter the network. That is, the unauthorized station now requests authentication to the network. In response, the AP sends a new challenge frame. This challenge frame will have a different content (since a new IV will be used to create the challenge) and a different CRC-32 check sum. The invader computes a valid CRC-32 check sum (see later discussion), encrypts the challenge with the key stream acquired earlier, appends the IV used and sends the frame.

While this authenticates the unauthorized user, the network cannot be used unless the shared key is also broken since only having access to a single valid key stream is not sufficient for further communication using the WEP algorithm. Methods for acquiring the secret key are described later.

RC4 Encryption

There is nothing inherently wrong with RC4. Unfortunately, WEP is not a secure implementation of RC4 and violates several other cryptographic design and implementation principles [WALK00].

Interception

In some cases attacks depend on the ability of an adversary to intercept wireless traffic. Fundamentally, we know that any traffic transmitted by radio signal is subject to interception since it is a radio frequency broadcast. The IEEE 802.11 standard specifies three possible physical layers, Infrared (IR), Frequency Hopping Spread Spectrum (FHSS), and Direct Sequence Spread Spectrum (DSSS) and broadcasts in three frequency bands, 900 MHz, 2.4 GHz, and 5 GHz. Most products currently being fielded use DSSS and the 2.4 GHz band. Interception is an easy matter even for relatively unskilled adversaries. That is because any commercial wireless device designed for service in the appropriate band of frequencies is readily capable of receiving all signals. It is then a relatively easy matter to modify device drivers and/or flash memory to promiscuously monitor all traffic. Consequently, it should be assumed that an adversary has access to intercepted signals.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Keystream Reuse

We have described the basic operation of RC4 as illustrated in Figure 1. One of the well known attributes of stream ciphers operating in output feedback mode is that encrypting two messages under the same IV and key can reveal information about both messages to a cryptanalyst. Consider the encryption of two plaintexts, P_1 and P_2 as follows:

$C_1 = P_1 \oplus RC4\ (IV, K)$, and

$C_2 = P_2 \oplus RC4(IV, K)$, then

$C_1 \oplus C_2 = (P_1 \oplus RC4\ (IV, K)) \oplus (P_2 \oplus RC4(IV, K))$

If the same IV and Key are used, then

$C_1 \oplus C_2 = P_1 \oplus P_2$

That is, the Exclusive OR of the two ciphertexts will produce the Exclusive OR of the two plaintexts. Thus, if the plaintext of one message is known, the plaintext of the other message is revealed. One way to achieve this would be for an attacker to send a known plaintext message to a wireless device and then intercept the encrypted message associated with the plaintext. While this raises a number of difficulties, it is a feasible attack.

The traffic must be intercepted and an adversary must find an instance of the same key and same IV being associated with one, or more, other messages (i.e., other than the one the adversary injected) on the network. Since the shared key is used by multiple stations the requirement for the use of the same key is satisfied. Consequently, the adversary must find messages using the same IV.

Reading the IV is trivial. The IV is transmitted in the clear (i.e., unencrypted) with every packet. Recovering an IV with the same value depends on how well IVs are initialized, how well they are constructed (e.g., the size of the IV space (length in bits)), and how often they are re-used in a typical network.

The standard recommends, but does not require, changing the IV for every frame transmitted. It provides no guidance on selecting or initializing the IV. The work at UC Berkeley indicates that some PCMCIA cards reset the IV to zero when initialized and then increment the IV by one for each packet transmitted [BORI01]. This is a relatively predictable pattern and it can be expected that a relatively higher proportion of low-valued IV's would appear on the network than would be expected in the IV's were randomly initialized.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The standard specifies the size of the IV field to be 3 octets (24 bits). If the IV is initialized to zero and incremented by one for each packet, it can be expected that the IV will roll over mod 24. That is, the IV will be re-used after 2^{24} packets have been transmitted from a station or an AP. MAC frames range in size from 34 Bytes to 2346 Bytes. Minimum rollover would occur at 2^{24} x 34 Bytes and maximum rollover at 2^{24} x 2346 Bytes or from about 570 MBytes to 40 GBytes (between 4.5 and 320 Gbits). This would be a large number for a single user station to transmit, but consider a busy access point. Since traffic is encrypted by the access point for transmission to multiple user stations the access point sends its IV with each packet. A fully loaded access point is capable of sending 660 Mbits per minute, 39.6 Gbits per hour, and 432 Gbits per day.

When rollover actually occurs depends of the traffic volume at the AP, the size of packets being transmitted, and the specific implementation of IV initialization and updating. In the Berkeley paper, the authors predict that a busy access point operating at half capacity would exhaust the IV space in about half a day [BORI01-4]. Walker predicts key space exhaustion in about an hour on a loaded access point [WALK00].

However, the reality is worse because of the birthday paradox. The birthday paradox is based on the counter-intuitive result that in a group as small as 23, the probability of two people have the same birth month and day is about 50% [STAL99]. That means that even if the IV were implemented as a random number, it is expected that a collision could occur after transmitting only 5000 packets [BORI01-5]. It increases to 99% after 12,430 frames [WALK00].

Many would consider a fully loaded network access point as an unlikely workload on most networks. The consequence is simple for lightly loaded networks. An adversary would have to be more patient for rollover to occur. The adversary also has another advantage. Given simple implementations of the IV, it is likely that IV collisions (i.e., an instance of equivalent keys and IVs) would occur as the result of new stations joining the network in the same initialized state.

In order to execute this attack the adversary would have to capture packets and compare IV values searching for collisions. A collision would allow analysis of a single packet. If the plaintext of one packet is known and is carefully selected, then the plaintext of the other packet would be revealed.

It is a relatively simple matter to get a known plaintext injected into the network by injecting a message from outside the network, but addressed to a mobile user on the network. Monitoring transmissions is somewhat more difficult, but can be done by operating a mobile device in promiscuous mode as discussed earlier. Once the key is revealed all transmissions using that key and IV are compromised.

The process is simplified to a great extent if the IV is not changed every packet. The standard recommends, but does not require, the IV to be changed every packet.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Integrity Assurance

The standard specifies an integrity algorithm that operates on the original plaintext message to produce an Integrity Check Value (ICV). The original plaintext is concatenated with the IVC to form the plaintext to be encrypted. The IVC method specified in the standard is CRC-32. The IVC is a 32-bit field called the FCS field and is defined as the last 4 octets in the MAC frame. Since the CRC-32 function is a linear function that uses only addition and multiplication, it is possible to change one, or more, bits in the original plaintext and be able to predict the bits to change in the CRC-32 checksum such that the checksum remains valid when it is received. Integrity methods that are cryptographically secure such as hash algorithms are non-linear functions that are not readily attacked. What this means is that it is possible to modify legitimate messages and insert them in the data stream without detection. This is probably not a concern for messages presented by the application for transmission. However, the checksum is performed over the entire MAC packet and that includes higher-level protocol routing address and port fields. If an adversary turns his or her attention to modification of the IP destination field, it is possible to re-direct traffic to an unintended destination under the control of the adversary. In addition, the capability to forge valid CRC-32 checksums is required to carry out the authentication attack described earlier.

Current Situation

Existing Products

In order to field a compatible implementation of the standard, vendors must implement all mandatory features of the standard. In some cases, like the use of CRC-32 for integrity, the standard is weak by design and needs to be changed. Until that happens, products will continue to be implemented with known weaknesses.

In other cases, stronger security measures are possible without violating the standard. Key management, for example, is a function that is external to the standard and can be implemented as a product developer sees fit. While this creates the issue of interoperability limiting the selection of products for the organization that desires stronger protection most vendors do offer options that strengthen security.

The point to be made is that specific products must meet the standard, but may be extended in various ways to improve security. Products are changing rapidly and the prospective implementer should be diligent about getting the most recent vendor information.

IEEE Activities

There continues to be on-going development of the standard and a part of that development is stronger security measures. The chairman of the IEEE 802 committee has publicly responded to the threat and vulnerabilities raised by the U. C. Berkeley team. Some of his more important comments are paraphrased as follows [KELL01]:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

1. WEP was never intended to provide more protection than a physically protected LAN environment. Since most LAN's are physically protected from external access, WEP was designed for equivalency protection from casual eavesdropping. WEP was never intended to be a complete security solution. Like wired LANs, a wireless network needs to be augmented with additional security mechanisms (e.g., end-to-end encryptions, virtual private networks, etc.), as appropriate to the requirements of the user organization.
2. The active attacks are not easy to mount. They are conceivable given enough time and resources, but may not yield enough value to an adversary to be worthwhile.
3. Since July 1999, task Group E of the standards committee has been working on extensions to the standard with the specific goal of strengthening the security of the standard. The enhancements currently being considered are intended to counter extremely sophisticated attacks, including those that have been recently reported in the press.

It will be sometime yet until the standard is modified, balloting is complete, and new protection mechanisms work their way into commercial products. However, the message is clear that the standard will change and new products will provide increased protection. What is not clear is whether it will be possible to upgrade equipment that has already been fielded.

The Intel Paper [WALK00]

Walker appears to have been the first to publish serious objections to the 802.11 standard. He argues that WEP is so seriously flawed that increased key sizes and strong key management will not protect the confidentiality of information transmitted over the network because WEP is fundamentally flawed. He argues for the replacement of the encryption algorithm, the addition of a session key derivation algorithm in shared key systems (not required in systems with dynamic keying), between pseudo-random number generation, lengthening the IV to 128 bits, adding a sequence number in dynamic keyed implementations to ensure keys are changed regularly, adds a 128 bit cryptographic integrity check, and encryption of addition elements of the payload.

The University of Maryland Paper [ARBA01]

The Maryland paper is the most recent and is consistent in arguing that the prevailing mechanisms specified in the standard are completely ineffective leaving them vulnerable to unauthorized entry and use. Consequently, they argue for a new encapsulation algorithm and the addition of cryptographically strong integrity measures.

The U. C. Berkeley Paper [BORI01]

The Berkeley paper is both a simple and complex document. Some of the attacks and vulnerabilities described are real and can be mounted with a moderate effort while others

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

are difficult and available to only a sophisticated attacker with significant time and resources. In essence, the document reports two significant weakness in wireless security:

1. The use of a shared key coupled with the use of a relatively short 24-bit Initialization Vector (IV) makes it possible with moderate effort to recover keys and decrypt encrypted communications. This also leads to more esoteric attacks, but they are harder to realize in practice.
2. The use of a CRC-32 checksum for integrity assurance instead of a cryptographically secure Message Authenticating Code places the integrity of messages at risk. This is not generally a concern associated with the disclosure of the contents of applications messages, but it establishes the possibility of an IP re-direction vulnerability that could compromise the entire network and also leads to unintended authentication attacks. The effort in this case is still moderate and the threat cannot be realized remotely. It requires that the adversary have proximate access to the radio communications of the wireless network. It also provides the opportunity for rogue stations to authenticate to the network. The effort in this case is relatively low. However, authentication alone does not enable use of the network. To use the network the authenticated station must also acquire the shared key.

In their concluding remarks, the writers describe several countermeasures that can be implemented. In general, these actions are also supported by other authors who have written about wireless security. They make the following recommendations:

1. As a first priority, the wireless network should be placed outside an organization's perimeter firewall as opposed to connecting behind the firewall.
2. For access between mobile stations attached to the wireless network and systems inside the firewall, they recommend the use of a Virtual Private Network.
3. The network should be configured to eliminate routes between the wireless network and the Internet. However, they do indicate that it may be desirable to allow visitors to access the Internet through the wireless network.
4. Finally, they recommend consideration of improvements in key management that results in every wireless station having its own encryption key and that the keys be changed frequently. Since this capability is external to the standard it does not affect compliance with the standard. However, it does increase the potential for interoperability failures and is likely to restrict product selection.

In addition, sites should consider the following:

- Develop a comprehensive WLAN policy, develop and document a WLAN architecture.
- Access a site's internal network from a wireless LAN should be protected at a layer above 802.11b data link protection (e.g., IPsec, Transport Layer Security, etc.) that implements strong authentication, confidentiality, and integrity services.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- If the WLAN is connected to the Internet, it should be protected from Internet-based attacks by appropriate perimeter protection (e.g., router filters, firewalls and/or intrusion detection).
- Protect portable devices that connect to multiple networks either concurrently or sequentially to avoid the introduction and transport of malicious code between networks.
- Do not use access control lists based on the client's Ethernet MAC address.
- Carefully consider radio frequency coverage when locating access points.

References and Bibliography

Borisov, N., I. Goldberg, and D. Wagner, "Security of the WEP Algorithm." URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (14 Nov. 01).

[ARBA01] Arbaugh, William A., N. Shanker, and Y.C. J. Wan, "Your 802.11 Wireless Network Has No Clothes." URL; http://www.cs.umd.edu/~waa/wireless.pdf (14 Nov. 01).

[BORI01] Borisov, N, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11." URL; http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf. (15 Nov. 01).

[BORI01-3] Borisov, N, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11." URL; http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf. Pg. 3. (15 Nov. 01).

[BORI01-4] Borisov, N, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11." URL http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf. Pg. 4. (15 Nov. 01).

[BORI01-5] Borisov, N, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," draft, available at http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf. Pg. 5. (15 Nov. 01).

[COX01] Cox, J., "High-speed wireless LANs are coming," Network World, April 9, 2001 (2001), 22.

[GILLI00] Gillian, S., "Vulnerabilities within the Wireless Application Protocol," August 31, 2000, URL: http://www.sans.org/infosecFAQ/WAP.htm (13 Nov 01)

[KELL01] Kelly, S. J., "Chair of IEEE 802.11 Responds to WEP Security Flaws." February 15, 2001. URL; http://slashdot.org/articles/01/02/15/1745204.shtml (15 Nov. 01).

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

[LAN99] LAN MAN Standards Committee of the IEEE Computer Society, "Wireless LAN Meduim Access Control (MAC) and Physical layer (PHY) specifications," ANSI/IEEE Standard 802.11, 1999 edition, 1999.

[ROSS00] Ross, B. J., "Containing the Wireless LAN Security Risk." November 4, 2000 URL; http://www.sans.org/infosecFAQ/wireless/wireless_LAN.htm (15 Nov. 01).

[STAL99] Stallings, William, "Cryptography and Network Security: Principles and Practice," 2nd edition, Prentice Hall, Upper Saddle River, NJ, 1999, 264-269.

[STUB01] Stubblefield, A., J. Ioannidis, and A. Rubin, "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP," AT&T Labs Technical Report TD-4ZCPZZ, August 6, 2001.

[WALK00] Walker, J. R., "Unsafe at Any Key Size: An analysis of the WEP encapsulation," doc.:IEEE 802.11-00/362, October 27, 2000, 9 pgs.

[WANG00] Wang, S., "Threats and Countermeasures in Wireless Networking," December 20, 2000, URL; http://www.sans.org/infosecFAQ/wireless/threats.htm (14 Nov. 01).

© SANS Institute 2001, Author retains full rights.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 4th, 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
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	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 Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 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
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced