GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Wired Equivalent Privacy Vulnerability

Princy C. Mehta

LevelOne Security Essentials Track, *April 2001*

Abstract

The Institute of Electrical and Electronics Engineers (IEEE) 802.11 is a standard for wireless local area networks (WLANs). To provide security features to an intrinsically insecure to transmit data, 802.11 introduced the Wired Equivalent Privacy (WEP) protocol, thereby trying to bring the security level of wireless systems to a similar level as their wired brethren. However, a group of researchers from the University of California at Berkeley and Zero-Knowledge Systems have exposed grave flaws with WEP's intended security goals [BO2].

The significance of this discovery cannot be overemphasized: hackers could intercept the transmission of data, read their contents, and modify them without detection. This paper will describe such vulnerabilities of WEP and how attacks can be mounted against it. It should be noted that a fellow *SANS Security Essentials* student briefly examined transmission security of wireless systems, advocating 802.11's encryption; however, its vulnerabilities have only been uncovered since [MCM]'s publication.

Introduction

The approval of the IEEE 802.11 standard for WLANs in conjunction with ongoing progress on increasing transmission speeds have made wireless systems extremely useful for businesses and consumers. Wireless systems offer users untethered network access, enabling mobile computing. As a result, wireless networks have gained much popularity recently – by the end of 2001, an estimated ten million 802.11 radios will be deployed [SAN]. Unfortunately, the added convenience of wireless access comes with new and significant problems, such as exacerbated security concerns. When transmissions are broadcast over radio waves, they can be easily intercepted and masqueraded. Thus, there is a great need to employ security mechanisms to protect wireless communications.

802.11 WLANs typically communicate between stations and access points (APs) using radio waves such that line-of-sight communication between the access point and wireless station is not required. The three physical layers defined in the standard include two spread-spectrum radio techniques and a diffuse infrared specification. The radio-based standards operate within the 2.4 GHz Industry, Scientific, and Medical (ISM) band. 802.11 defines data rates of 1 Mbps and 2 Mbps via radio waves using frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS). 802.11b is an enhancement of 802.11 employing DSSS to achieve a maximum throughput of 11 Mbps. Exploiting this throughput plays a key role in one of the attacks, as will be evident when Equation 1 is discussed later in the paper.

Along with the specifications of transmission, 802.11 defined the WEP protocol to address some of the security issues. The principal goal of WEP is to defend the confidentiality of data from eavesdroppers. Another objective is to guard against surreptitious modification of data (integrity). An ancillary intention of WEP is to provide access control to the WLAN

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

infrastructure. Regrettably, with the vulnerabilities discovered by the researchers, WEP's security goals can be defeated. WEP employs the well-known Ron's Code 4 Pseudo Random Number Generator (RC4 PRNG) algorithm –a symmetric key encryption algorithm from RSA Security, Inc. [GRO] – but still contains major security errors. These flaws permit several passive and active attacks that allow eavesdropping on and modifying wireless transmissions.

The WEP protocol will be concisely summarized next. Proceeding that will be explanation on each of the four attacks that exposed WEP's vulnerabilities. The paper will conclude by suggesting why a more in-depth study was not conducted before finalizing the WEP protocol in 802.11 and will offer workaround solutions to counter these attacks.

The WEP Protocol Architecture

802.11 defines an optional WEP mechanism to provide confidentiality and integrity of traffic in the WLAN. WEP is used at the two lowest layers of the Open Systems Interconnect (OSI) reference model, data link and physical layers; thereby, it does not offer end-to-end security. WEP depends on a secret key shared between the communicating parties (mobile station and AP) to protect the payload of a transmitted frame in each direction. Moreover, the RC4 PRNG algorithm used by WEP includes an integrity check vector (ICV) to check the integrity of each packet. This process is summarized below.

First, WEP computes the ICV by performing a 32-bit cyclical redundancy check (CRC-32) of the frame and appends the vector to the original frame, resulting in the plaintext. Then, the message plus ICV is encrypted via the RC4 PRNG algorithm using a long sequence key stream– a long sequence of pseudorandom bits. This key stream is a function of the 40-bit secret key (which is shared between all authorized stations in the WLAN) and a 24-bit initialization vector (IV). Consequently, an exclusive-or (XOR) operation is made between the plaintext and the key stream to produce the ciphertext. Finally, it is the ciphertext that is sent over the radio link. Theoretically, the ciphertext provides data integrity because of the ICV and confidentiality due to encryption.

The receiver, inasmuch as RC4 PRNG algorithm is symmetric, performs the same procedure described above, but in reverse, to retrieve the original message frame. Specifically, the ciphertext is decrypted using a duplicated key stream to recover the plaintext. The recipient then validates the checksum on this plaintext by computing the ICV and comparing it to the last 32 bits of the plaintext, thus ensuring that only frames with a valid checksum will be accepted by the receiver.

WEP can be implemented with the classic 40-bit key and 24-bit IV or a vendor-dependent (hence proprietary) extended version that affords a larger key. The shorter key length can be relatively easy to compromise via brute-force attack, even with modest computing resources; however, a larger key such as the 128-bit keys would be render brute-force attacks impossible, even for sophisticated computing systems. Nevertheless, alternative attacks are possible that do not require a brute-force strategy, thereby diminishing the strength of key length.

The subsequent four sections describe each of the potential attacks.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Passive Attack to Decrypt Traffic

As mentioned, the IV is a 24-bit field intended to randomize part of the key (since the 40-bit key is shared by all stations on a WLAN). This means that an 802.11b AP transmitting at 11 Mbps can exhaust all IV combinations within 5 hours, as shown in Equation 1.

$$\frac{1500\ bytes}{packet} \times \frac{8\ bits}{1\ byte} \times \frac{1\ \text{sec}}{11\ Mbits} \times \frac{1\ Mbit}{10^6\ bits} \times 2^{24}\ packets \approx 18{,}300\ \text{sec} \approx 5\ hrs$$

Equation 1: Time to Exhaust 24-bit IV

While 802.11b APs generate a theoretical maximum of 11 Mbps, its observed rates are usually much less due to overhead and packet collisions, which can increase the amount of time before an IV is reused. However, packets are usually not at the Ethernet maximum of 1500 bytes, which reduces the IV reuse. In any event, this small space of IVs *guarantees* that a key stream will be reused in less than one-half of one day.

The importance of this relatively small time is that an attacker can collect two ciphertext packets that are encrypted with the same key stream. Then he can perform statistical attacks to recover the plaintext, and once has positively matched a ciphertext message with its plaintext counterpart, then an XOR operation will reveal the key, enabling him to comprehend all other ciphertext messages. Hence, it is fruitful for the passive eavesdropper to intercept all wireless traffic until an IV collision is observed.

Even if the threat cannot understand all of the contents, he can infer them by exploiting the predictable nature and redundancy of IP traffic. Further educated guesses about the contents of a plaintext message also allows the threat to statistically diminish the space of possible messages to get a clearer idea of the exact contents. As the attacker ascertains more collisions using the same IV, he can get an even better understanding of the concealed messages, facilitating the success rate of statistical analysis.

A variation to this attack that a threat can use a host to send traffic from outside the WLAN to the AP. Once he taps its ciphertext from the air, since he knows the plaintext (which he fabricated) and now the ciphertext, he can recover the crucial key stream.

Active Attack to Insert Traffic

The problems from the attack mentioned above can be worsened. If an attacker knows the precise plaintext and ciphertext pair, he would manifestly be able to generate the key stream. With this knowledge, the threat can build correctly encrypted packets by constructing a message, calculating its CRC-32, and executing an XOR operation with the newly-discovered key stream. This ciphertext packet can be sent to the AP or mobile station to deceive it into thinking that it is a valid packet.

A minor modification to this attack can make it much more pernicious. Even if the threat has not attained complete knowledge of the packet, he can alter selected bits of the message and

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

successfully adjust the encrypted ICV to obtain a correct encrypted version of the modified packet. This is a lethal attack of the packet's integrity, since all the attacker requires is partial knowledge of the packet's contents to perform selective modification.

Active Attack from Both Ends

The above active attack can be extended even further to decrypt arbitrary traffic. Suppose the attacker speculates about the frame's header only, not necessarily its actual contents. For example, the threat may be able to predict the destination IP address with a high degree of confidence. Equipped with just this information, the attacker can modify appropriate bits to transform the destination IP address to send the packet to a machine in his control via a rogue mobile station. Then the packet could be successfully decrypted by the AP and forward as plaintext to the attacker's machine for the attacker to enjoy.

Even if the AP is cloaked behind a firewall, if the attacker can deduce the TCP headers of the packet, he can change it to port 80 (generally indicating World Wide Web service), thereby allowing it to be forwarded after decryption through most firewalls and to his machine somewhere on the Internet.

Table-Based Attack

The small space of potential IVs can allow the threat to construct a decryption table. Once the plaintext of a packet is realized, an attacker can compute the key stream produced by the IV utilized. Accordingly, this key stream can be used to decrypt all other packets employing the same IV. Eventually, the threat can generate a table of IVs and corresponding key streams. Then the black hat can decrypt any and *all* packets sent over the wireless link, regardless of their IVs.

Because the table can contain up to 2^{24} (over 16 million) values, and each entry is a maximum of 1500 bytes, the table will be no larger than 24 GB. Thus, it is conceivable that a committed attacker can accumulate enough data to build a full decryption "dictionary". While this would be an arduous undertaking, his motivation is that once the table is formed, it is possible to immediately decrypt every subsequent ciphertext with little effort. Worse yet, this table can be distributed to other black hats. The flaw herein lies in the 24-bit IV; if the IV is expanded in a future version of WEP, constructing such a dictionary would be exponentially more laborious.

WEP Blame Game

It appears that the fault of the recently revealed vulnerabilities of WEP falls squarely among the WEP architects. Ostensibly, the technical specifications were not open to peer review and might have fell victim to "security through obscurity" – the false belief wherein if hiding the specifications would keep it more secure, the less likely the algorithm would be cracked. Since they allegedly did not invite cryptanalysts to the review, the algorithm did not endure rigorous testing, which led to elementary mistakes in the cryptography. This could be due to the apparent conflict of interest in that people working on the standard are also working for companies developing proprietary and/or workaround solutions [FIS]. Thus, WEP became a de facto

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

standard of these firms instead of going through a stricter public review. WEP's gaffes underscore how much of the industry's wireless infrastructure was standardized and built without paying careful attention to security.

Another enormous misjudgment that can now compromise integrity was in the selection of checksums via CRC-32 to perform integrity checks. [BO1] demonstrated the importance of using a cryptographically secure message authentication code (MAC), such as SHA1-HMAC, to protect the integrity of transmissions. The use of CRC is inappropriate for this purpose since an attacker simply needs to flip selected bits of a message to yield the same ICV as the original one. A secure MAC is especially essential when considering a composition of protocols because the lack of message integrity in one layer of a system can breach secrecy in the larger system.

As far as the selection of the encryption algorithm itself, the RC4 PRNG algorithm, extending the key length may effectively mitigate brute-force attacks. However, the 802.11 Chair of WEP Security countered that the choice of encryption algorithms by the 802.11 group were not purely technical decisions but were limited by the US government export law restrictions [ZUR]. This explains why domestically, vendors are promoting their proprietary 128-bit solutions. While this may provide stronger encryption security, it would sacrifice the original intent of the standard: to allow interoperability of 802.11-compliant equipment from different vendors. This is a classic tradeoff between functionality and security.

Workaround Solutions

Now that the flaws have been exposed, there are suggestions on allaying the 802.11 vulnerabilities. The best solution is for administrators of an 802.11 WLAN to practice defense in depth. That is, multiple security measures should be implemented, so even if the threat can exploit WEP's vulnerabilities, other security measures will thwart his additional effort. For example, the WLAN should be placed outside the firewall to run a virtual private network (VPN) to the inside of the firewall. The Remote Authentication Dial-In User Service (RADIUS) protocol can be implemented to provide another level of security designed to authenticate remote clients to a centralized server [SHI]. Even better, the system should employ end-to-end encryption.

It is not encouraging to hear, "Our wireless networks are absolutely more vulnerable than our wired ones are", as said by Professor David Wagner of the University of California at Berkeley, one of the researchers who discovered WEP's flaws [FIS]. The problems with WEP are not expected to be resolved for at least six months to one year. A task force within the IEEE is working on upgrading WEP to WEP2 with the intention of separating encryption and authentication functions so that the same static key does not need to be shared within a WLAN. Unfortunately, the follow-on algorithm is again arriving from vendors trying to control the process rather than letting the best solution emerge [HOL]; politics, rather than technical merit, may once more control WEP's direction.

Recognizing that WEP2 will not be the WLAN's security panacea, the IEEE Task Group E has approved a draft to establish a stronger authentication and 128-bit key management system, tentatively called Enhanced Security Network (ESN). ESN's encryption will augment the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

weaker RC4 PRNG algorithm with Advanced Encryption Standard (AES) [GAR]. ESN is not expected to be finalized until 2002, but it may achieve WEP's raison d'être: to provide a comparable level of security as a wired network.

Conclusion

Millions of users freely use 802.11 WLANs as an alternative to wired LANs, thereby achieving mobile computing. With this freedom comes conspicuous security concerns. Security must be infused in the process of any system; it cannot be an afterthought. It is disturbing to see how little consideration is given to something as important as security, as was exposed by the WEP vulnerabilities! As weak as WEP has proven to be, it is still better than not using any encryption to keep the casual passerby from tapping into the WLAN, albeit, it will only be an impediment to a determined black hat.

The good news is that countermeasures are available, and it forces administrators to employ defense in depth by not depending on just one security mechanism. In spite of WEP's failure of protecting two of the three fundamental pillars of security, confidentiality and integrity (WEP was not intended to support availability), perhaps its anticipated evolution, ESN, will be able to provide sufficient security to reduce risk to an acceptable level.

References

[BO1] Borisov, Nikita; Goldberg, Ian; and Wagner, David. *Intercepting Mobile Communications: The Insecurity of 802.11*. January 2001.

[BO2] Borisov, Nikita; Goldberg, Ian; and Wagner, David. *Security of the WEP Algorithm*. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html, University of California at Berkeley, February 2001.

[BOW] Bowman, Lisa M. *Wireless Networks Leave Holes for Hackers*. http://news.cnet.com/news/0-1004-201-4722179-0.html?tag=owv, CNET News.com, February 5, 2001.

[FIS] Fisher, Dennis and Nobel, Carmen. *Wireless LAN Holes*. http://www.zdnet.com/eweek/stories/general/0,11011,2684337,00.html, eWeek, February 11, 2001.

[GAR] Garcia, Andrew. WEP Remains Vulnerable. http://www.zdnet.com/eweek/stories/general/0,11011,2700806,00.html, eWeek, March 26, 2001.

[GRO] Grogans, Candance; Bethea, Jackie; and Hamdan, Issam. *RC4 Encryption Algorithm*. http://www.ncat.edu/~grogans/main.htm, North Carolina Agricultural and Technical State University , March 5, 2000.

[HOL] *Holes in Wireless Nets*. http://www.zdnet.com/eweek/stories/general/0,11011,2687518,00.html, eWeek, February 26, 2001.

[MCM] McMurry, Mike. *Wireless Security*. http://www.sans.org/infosecFAQ/wireless/wireless_sec.htm, January 22, 2001.

[PES] Pescatore, John. *Commentary: An Object Lesson in Managing Security Risks of New Technologies*.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

http://www.techrepublic.com/article.jhtml?src=search&id=r00120010207ggp10.htm, TechRepublic, Inc. February 7, 2001.

[SAN] Sandberg, Jared. *Hackers poised to land at wireless AirPort*. http://www.zdnet.com/enterprise/stories/main/0,10228,2681947,00.html, ZDNet, February 5, 2001.

[SHI] Shim, Richard. *How to Fill Wi-Fi's Security Holes*. http://www.zdnet.com/enterprise/stories/main/0,10228,2693864,00.html, ZDNet, March 8, 2001.

[USK] Uskela, Sami. *Security in Wireless Local Area Networks*. http://www.tml.hut.fi/Opinnot/Tik-110.501/1997/wireless_lan.html, Helsinki University of Technology, 1997.

[ZUR] Zurko, Ellen. *Listwatch: Items from Security-Related Mailing Lists*. http://www.ieee-security.org/Cipher/Newsbriefs/2001/022001.ListWatch.html, IEEE, February 16, 2001.

[ZYR] Zyren, Jim and Petrick, Al. *IEEE 802.11 Tutorial*. http://www.wirelessethernet.org/whitepapers.asp.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.