Karen L. Duez. Wireless Security: What Technology Is the Most Secure? A Master's paper for the M.S. in I.S. degree. May, 2003. 34 pages. Advisor: Greg Newby

This paper looks at the security of wireless networking solutions. The study focuses on current wireless security standards and technologies and points out the problems that these face. A variety of wireless security solutions are looked at and discussed.

The future technologies show promise as far as fixing the mistakes of previous wireless security technologies. Although, as in all security areas, in the end there is not one solution that is secure for every circumstance.

Headings:

Wireless communications systems – Security measures

Local Area Networks (Computer networks) – Standards

Computer networks – Security measures

WIRELESS SECURITY: WHAT TECHNOLOGY IS THE MOST SECURE?

by

Karen L. Duez

A Master's paper submitted to the faculty of the School of Information and Library Science of the University of North Carolina at Chapel Hill in partial fulfillment of the requirements for the degree of Master of Science in Information Science.

Chapel Hill, North Carolina

May 2003

Approved by:

_____

Dr. Greg Newby

Table of Contents

Introduction

This paper will provide a look into the wireless networking security field. "The very nature of most wireless communications makes security a significant factor that must be understood and addressed for wireless communications to achieve its vast potential" (Nichols and Lekkas 10). Information security, as a whole, is a hot field at the moment, as more and more corporations, governments, schools and even home users are trying to protect their valuable information from those who might try to misuse or destroy it. What will be addressed in this paper includes the current shortcomings with wireless security and the products and standards that are being created to overcome these pitfalls. This information is vital to anyone who uses a wireless LAN -- at home, school or work.

The world is not always a safe place and everyone needs to be aware of the fact that there are people out there who may try to access information that does not belong to them, and wireless is an extremely open technology. There are new vulnerabilities with wireless networking because radio waves cannot be stopped by physical boundaries, but all the wired networking risks are there, too (i.e. DoS attacks, man-in-the middle attacks, password theft, port scanning, etc.) These well-known attacks have been adapted to a wireless technology, in addition to new threats. "Wireless has in fact fewer physical assets to protect, but, at the same time, there is no locked door on the airwaves so it is far easier to *hack*" (Nichols and Lekkas 2).

The focus of this paper is going to be on how security is implemented in the IEEE 802.11 standard for wireless. Wired Equivalency Protocol (WEP) was included as part of the original 802.11 standard. Several teams soon developed studies to prove that WEP was easily crackable. The Institute of Electrical and Electronics Engineers (IEEE) has repeatedly claimed that WEP was intended only to be as secure as a wired network would be, not more. WEP will be explained in more detail in the next section.

The other wireless networking technologies have experienced similar difficulties in achieving the level of security necessary to make corporations comfortable with general deployment. Bluetooth Special Interest Group Executive Director Mike McCamon has expressed that they are very concerned about security. He says, "We use frequency hopping and 128-bit encryption in addition to other known methods to enhance our technology." (Behr and Butterfield 1). Additionally, the technology is short-ranged, so the interloper would need to be within the 30 feet limitation to cause any damage.

Wireless networking has become the wave of the future for Local Area Networks (LAN). It offers the advantages of mobility, ease and speed of deployment, flexibility, and, over the long run, less expensive costs. The purchase and installation of wireless equipment may be expensive at the outset, but it is much easier and cheaper than running wire, especially in the case of historical buildings where protection forbids certain types of

construction to be done. Plus, leasing capacity from ISPs or telcos is extremely expensive, so having wireless technology eliminates the need to do this.
Initially, the limitations of speeds (802.11 standard) of only 1 to 2 Mbps seem to be a big downside to using wireless, as compared to wired networking. These speeds are getting better as more equipment comes out as a result of the standards being released. Now speeds of up to 54 Mbps are possible.

There are several different types of wireless networking that are emerging almost in unison. They vary from IEEE standards to Bluetooth to HomeRF. I will mention a few in brief, but the focus of the paper is going to be the Institute of Electrical and Electronics Engineers (IEEE) standard, 802.11.

Bluetooth

Bluetooth works on the 2.45 GHz frequency. It uses spread-spectrum frequency hopping technology, so a Bluetooth device will use 79 individual, randomly chosen frequencies and change from one to another on a regular basis.

The basic principle behind Bluetooth is to allow any sort of electronic device like keyboards and headphones to 'make' their own connection wireless, without having to worry about which cable connects to which port. Bluetooth is not only a standard for the physical connection, but also the next level up (when bits are sent, how many will be sent at one time and also an integrity check to make sure what is sent is the same as what is received.)

The range of Bluetooth is quite small, about 10 meters, because the devices send out very weak signals of 1 milliwatt. This quality helps Bluetooth devices to avoid interference with other kinds of devices within the same frequency.

The most unique characteristic of Bluetooth devices is how they begin their communication. Initially, when two devices come within range of one another, they have a conversation to determine whether they have data to share or if one needs to control the other. The devices that need to communicate will create a Personal-Area Network (PAN) or piconet, which can fill the space of a room or be between two devices very close together. Once this piconet is established, the members will randomly hop frequencies in

unison to avoid interference, as that frequency is already susceptible to interference from many small electronic devices, like microwaves.

Another advantage of Bluetooth is that it is designed to work in both half-duplex and full-duplex modes. In full-duplex mode, a Bluetooth device can transmit data at more than 64,000 bits per second. (Franklin 6).

HomeRF

HomeRF, which stands for *home radio frequency*, was developed by Proxim Inc. An alliance of businesses has since backed this standard, calling it Shared Wireless Access Protocol (SWAP). It is a home wireless networking standard that combines 802.11b and Digital Enhanced Cordless Telecommunication (DECT) into a single system. This technology uses a frequency-hopping technique to deliver speeds of up to 1.6 Mbps over distances of up to 150 feet. One advantage that HomeRF has over Wi-Fi (802.11 standard) is that it has better mechanisms in place to deal with interference and also to handle voice, video and audio, because it includes six voice channels based on the DECT standard.

Another advantage of SWAP is that the prices of SWAP devices are lower, as SWAP is geared toward the home user and no access point is required to implement it. This may not make a difference in the long run, as corporations implement other wireless technologies, and the users want to bring the work wireless technology home with them. Plus, the speed of SWAP is significantly slower than 802.11. In 2000, the Federal

Communications Commission (FCC) ruled that HomeRF standard allowed for an increase in transmission speeds from 1MHz to 5 MHz, which means that this services can be as fast as the 11Mbps of Wi-Fi (Batista 1).

WECA opposed this ruling because it claims that this increase in bandwidth given to SWAP could create more airwave interference, thereby slowing down Internet connections overall.

There is also a HomeRF 2.0 supposedly going to be released, as pushed by Proxim Inc. The standard includes support for up to four voice wireless phone headsets. This version will include the increased speeds that the FCC ruling allowed, for up to 10 Mbps (same is standard wired Ethernet speeds). Plus, the new standard will have new security features, interference dodging features and quality of service (QoS) features. HomeRF 2.0 will be backwards compatible with version 1.0 and hopefully will roll out support for 20 Mbps by 2003 (Kaminski 1).

From an April 2002 article from weblogger.com, the end of HomeRF may be in sight. The foundation of the HomeRF standard was that it included data, telephony, and multimedia in its inception. Unfortunately, the speeds lagged behind due to the late-coming FCC decision. Initially, HomeRF did not see itself as a competitor to Wi-Fi because it was a geared to the home user, but now that 802.11b seems to be making its way everywhere, including the home, HomeRF has found itself to be too little too late.

802.11

802.11 is sometimes referred to as “wireless Ethernet” because the core elements are similar. Stations have 48-bit MAC addresses; the frames are delivered based upon MAC address; and frame delivery is unreliable. This technology uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), which differs from the CSMA with Collision Detection typically utilized by Ethernet. The reason is that the collision detection process tends to waste valuable transmission capacity. It is also unusual for wireless devices to receive and transmit simultaneously. The standard also included specifications to allow frames to be fragmented, in an attempt to increase the probability that the frames will be delivered without errors induced by interference. Interference for 802.11 (particularly 802.11b) can come from many electronic devices, like a microwave or cordless telephones, which utilizes the same frequencies.

The standard for wireless Ethernet 802.11 was released in 1997, with 802.11a and 802.11b emerging by 1999. The hardware was not built right away for the 802.11a standard, but has flourished for the 802.11b standard. 802.11g is nearly a standard, though as of yet, no equipment has been released.

The 1997 standard, IEEE Std. 802.11-1997 specified three physical layers that could be used: infrared (IR) baseband, frequency hopping spread spectrum (FHSS) radio in the 2.4 Gigahertz (GHz) range, and direct sequence spread spectrum (DSSS) radio in the 2.4 GHz band. Later, the standard included two new physical layers. 802.11a uses the orthogonal frequency domain multiplexing (OFDM) radio in the UNII bands. 802.11b

extends off the DSSS 2.4 GHz physical layer, using High Rate, Direct Sequence Spread Spectrum (HR/DSSS) instead.

802.11b has flourished so quickly because of the efforts of the Wireless Ethernet Compatibility Alliance (WECA). This alliance among major computing companies including Microsoft, Cisco, Intel, 3Com and many others, has led to the rapid adoption of "wireless fidelity" or Wi-Fi. "WECA's mission is to certify interoperability of Wi-Fi (IEEE 802.11) products and to promote Wi-Fi as the global wireless LAN standard across all market segments." (Gordon). With these major companies supporting the interoperability movement, it allows customers to feel confident that they will not get locked into a proprietary solution, which will never be compatible with other vendors, just in case they want to change in the future.

802.11b is typically fast (11Mbps), reliable, long range (1,000 feet in open areas, 250-400 feet in closed areas), can integrate well with existing wired-Ethernet networks, and is compatible with the original 802.11 DSSS devices. It is an improvement on the original 802.11 equipment, that generally only got 1-2 Mbps speed, was short ranged at 75-125 feet, walls interfered with communication, and it was difficult to integrate with existing wireless networks. 802.11b devices have tended to be more expensive, but with the support of WECA, and larger production and more vendors, prices have dropped significantly.

As 802.11b products were released before 802.11a, it was widely believed that the most logical move would be from 802.11b to 802.11a (from 11 Mbps to 54 Mbps). This would also be a move from the crowded 2.4 GHz band of the radio spectrum to the less crowded 5 GHz band. Other drawbacks to 802.11b technology are the lack of interoperability with voice devices and no quality of services provisions for multimedia content.

802.11a is now being promoted by WECA, also, under the nickname Wi-Fi5 (5 GHz, that is). WECA is again calling for interoperability among manufacturers, and hoping that at least two chip manufacturers will appear and at least three different vendor solutions. Hopefully, if this scenario occurs, the prices will lower and the technology will no longer seem "bleeding edge", thus seeming more stable to corporate buyers.

According to an informal comparison, done by Bruce Brown of extremetech.com, he found 802.11a to be almost five times faster than 802.11b at short distances (Brown "802.11a" 1). Although 802.11a and 802.11b devices are not compatible (5 GHz for 802.11a, 2.4 GHz for 802.11b), they can coexist within the same network, without causing interference. This may allow the two technologies to continue to exist side-by-side for the time being.

With 802.11a, the frequency of 5 GHz, provides an additional advantage over 802.11b. There are eight channels that can operate simultaneously in the two lower bands of the 5 GHz spectrum, as opposed to three for 802.11b.

Like 802.11b, there is still no support to optimize voice or multimedia content.

There is a standard being worked out still, 802.11g, which is compatible with 802.11b, but with a 54 Mbps data rate. It also operates at the 2.4 GHz range, so would continue to suffer from the interference problems of 802.11b. This move might be advantageous to organizations that have already deployed 802.11b equipment, but would like to upgrade their speeds.

Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) is the security protocol defined in the 802.11b standard, to overcome the added security risks that are associated with using a wireless network. The purpose of WEP is to ensure Wireless LAN systems have a level of privacy that is "equivalent" to a wired LAN by encrypting the data carried over the radio waves. Wired networks have a limited boundary that can be kept guarded by locks on doors and controlled entrances to buildings, whereas wireless may penetrate beyond any physical boundaries. WEP creates a "wall" for wireless, which merely acts as a first line of defense against casual intruders (WEP Security Statement).

The usage of WEP was intended to provide three security goals: confidentiality, access control, and data integrity (Borisov, Goldberg, Wagner 2). Confidentiality is achieved via the encryption of the data. Access control is provided as the users are required to authenticate to the access points with the shared key. And integrity was achieved by insuring that the data had not been tampered with, as an "integrity check sequence" is included with the protocol (Gast 89).

WEP uses a shared secret system between a wireless station and the access point that it is associated with. WEP is based on the well-known symmetric (meaning the algorithm uses the same key to encrypt and decrypt) stream (algorithm that encrypts data one byte at a time) cipher RC4 to encrypt the data in the packets. RC4 was developed in 1987 by Ronald Rivest, for RSA Data Security (RC stands for Ron's Code) and kept as a trade secret, until it was leaked out in 1994 (RC4 Encryption Algorithm 2). The protocol

specifies a 64-bit stream cipher, though some vendors have decided to provide a 128-bit cipher instead, as it may be more secure (Schenk, Garcia and Iwanchuk 12).

RC-4 uses a stream of bits, called a keystream, which is combined with the plaintext via an exclusive OR to produce a ciphertext. The ciphertext is processed by the receiver in combination with the shared key to recreate the original message. The transmission includes an initialization vector (IV) in conjunction with the ciphertext over the radio link, which means only the data in the payload of the frame is encrypted, whereas the MAC header is unencrypted (including the IV). In general, the WEP key is 40-bits (based on the US Government restriction on export of cryptographic technology), while the IV is 24-bits (this breakdown can also vary by vendor implementation). The following diagram shows the WEP process for encrypting data.

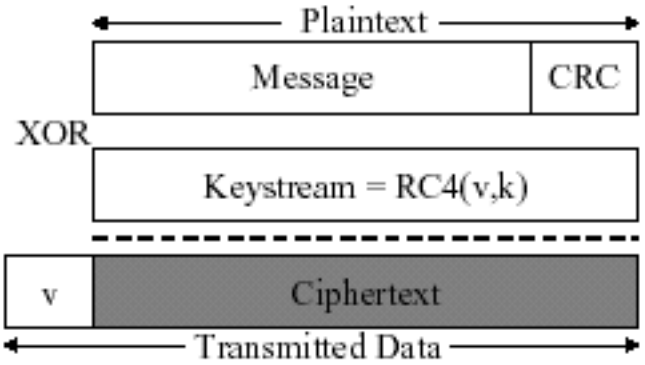

Figure 1: Encrypted WEP Frame.

(Borisov, Goldberg, Wagner 2).

To decrypt the packet, the recipient simply reverses the process shown in the diagram.

"WEP was initially marketed as the security solution for wireless LANs, though its design was so flawed as to make that impossible" (Gast 86).

As the above quote mentions, WEP quickly became out of favor in the world of wireless security. In one well-known study from August 2001, "Weaknesses in the Key Scheduling Algorithm of RC4", the final outcome of the paper was to say that "RC4 is completely insecure in a common mode of operation which is used in the widely deployed Wired Equivalent Privacy protocol (Fluhrer, Mantin, Shamir 1). The RC4 algorithm implementation in WEP was easily cracked, because the 40-bit key was short enough that brute-force attack are practical to anyone with relatively high powered computing resources (Borisov, Goldberg, Wagner 3).

A study done by Borisov, Goldberg and Wagner found these vulnerabilities of the WEP protocol to attacks:

1. Passive attacks to decrypt traffic based on statistical analysis.
2. Active attacks to inject new traffic from unauthorized mobile stations, based on known plaintext.
3. Active attacks to decrypt traffic, based on tricking the access point.
4. Dictionary-building attack that, after analysis of about a day's worth of traffic, allows real-time automated decryption of all traffic. (1).

The three basic goals of WEP were not met: confidentiality was compromised by the flaws in the RC4 cipher, the integrity check was poorly designed and the authentication

method was for users' MAC addresses, not to users themselves (so a misplaced wireless card could be used by anybody) (Gast 89). As more and more studies were done that pointed out the many flaws of WEP, a new wireless security model was needed . Wi-Fi reiterated that WEP was intended to make wireless have the equivalent security of a wired network, nothing further. This is not what larger companies wanted to hear. Corporations had already begun deploying this wireless technology into their campuses and now they learned that someone sitting in their parking lot with a fast-processor in a laptop with a wireless card, could intercept their valuable data. People were downloading "AirSnort" just to play around with it. "AirSnort is a wireless LAN (WLAN) tool, which cracks encryption keys on 802.11b WEP networks. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered" (from sourceforge.net). A new security standard was going to take awhile, but something had to be done in the interim.

The vendors themselves tried to come up with ways to make WEP more secure. As stated before, some came up with 128-bit RC4 encryption schemes. Also, some tried to include user-based authentication instead of the MAC address.

Evolution of Wireless Security

One security solution that has evolved as a result of the problems with WEP is based off of a previous IEEE standard, 802.1x, and adapted to the wireless LAN world. As of yet, a new wireless security standard has not been released, but as this idea is based off of previous standards, many vendors have accepted 802.1x, while they wait for the 802.11i standard to be finalized. In essence, it has become a de-facto standard. 802.1x is an authentication model at layer 2, which provides for port-based network access controls. This standard "provides a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics and of preventing access to that port in cases in which the authentication and authorization fails" (IEEE 3). "It translates messages from an authentication algorithm into the appropriate frame formats of wireless or wired LAN access types" (Wexler, "Is Cisco LEAP-frogging" 1).

The 802.1x protocol is divided into three different roles to insure the user attached to the physical port is supposed to have access to that network. These three parts are: the supplicant, or client attempting access to the network; the authenticator, or layer 2 device that the client is connecting to (in the wireless world an access point); and the authentication server, or the device that verifies the authentication data provided by the supplicant (Potter and Fleck 157).

The new security architecture works along with the IETF's PPP Extensible Authentication Protocol (EAP) – RFC 2284 to be the actual authentication protocol for the 802.1x transactions. According to the IETF standard, "EAP is a general protocol for

PPP authentication which supports multiple authentication mechanisms" (RFC 2284, section 2). It is a challenge-response type authentication and can use any crypto system to handle verification (Potter and Fleck 157).

The 802.1x process for authentication using EAP in a wireless scenario is made up of a series of steps that force the supplicant to prove that it should have access to the network. First of all, the supplicant sends an EAP-start message asking whether it has permission to access the network. Next, the authenticator responds to the start message with an EAP-request identity message, asking the client to prove whom it is. The supplicant responds with and EAP-response packet, which is forwarded to the authentication server. The server then uses an authentication algorithm to verify the supplicant's identity, which can vary depending on the implementation of 802.1x. The authentication server then sends a response of "reject" or "accept" to the authenticator, which prompts the authenticator to send an EAP-success (or reject) packet to the supplicant. At this point, if the supplicant is accepted, the access point will forward the traffic from and to the client as necessary. The supplicant has been accepted to the network. (Geier 1).

One downside of using EAP alone as the authentication method used by 802.1x, is that though it provides flexibility, it also unfortunately might allow the entire EAP conversation to be sent as clear text" (Microsoft 1). This sparked research into combining EAP with something else, which led to several different EAP-type authentication methods. Three of them will be discussed here: Cisco's LEAP, EAP-TLS and EAP-PEAP.

Cisco Systems, Inc, came up with one vendor implementation of this security model in November 2000. Cisco came out with the proprietary LEAP (Lightweight EAP), which it recently shared with Apple and other vendors to allow interoperability of products. LEAP works with the ideas of mutual authentication, protecting corporations against "rogue" Access Points; dynamic, session-based encryption keys; centralized user administration using a RADIUS server; and extensible authentication support. The process that to authentication is very similar to what was described above, but includes a proprietary "Cisco LEAP algorithm" for sending the encrypted keys that distinguishes it from other implementations (Wexler "Is Cisco LEAP-frogging" 1).

There are other EAP implementations that have been released as well. EAP-TLS (RFC 2716), or Transport Layer Security, is a certificate-based standard. This is also based on the idea of mutual authentication. As of yet, EAP-TLS is not widely used as a wireless security implementation, and is used only with Microsoft Operating Systems. In this case, a Certificate Authority (CA) server must be deployed in the network, which seems to make it difficult to troubleshoot and to install. EAP-TLS uses Public Key Infrastructure (PKI), an asymmetrical algorithm (Doshi). EAP-TLS is based upon Secure Sockets Layer (SSL) Version 3.0, with the SSL handshake performed over EAP (instead of TCP as on the Internet).

PKI provides protection of data. PKI authenticates identity, but using digital certificates to validate the identity of users. It also verifies integrity of the data by insuring that the

data has not been corrupted or changed in transit. PKI also insures that information is not intercepted during transmission. It authorizes access and transactions, which are important to the protection of information ("Extensible"). Drawbacks to PKI include: PKI systems tend to be CPU intensive on the client machine, they require careful planning and administration and they may be costly (Nichols and Lekkas 381).

The EAP-TLS model works similarly to the general process described above, but differs from LEAP in that the authentication is certificate-based, not password based. Additionally, EAP-TLS is not a proprietary solution, as the model was sent to the IETF by a collaboration of Cisco, Microsoft and other vendors.

Another EAP based wireless security solution is EAP-PEAP, or Protected EAP, which is a hybrid using both password and certificates for authentication (Doshi). This is also an extension to EAP and it allows the use of any of the secure authentication methods used with EAP (Riley 27). PEAP uses TLS as an enhancement to other authentication methods to provide a secure channel that is both encrypted and integrity-protected (Microsoft 1).

Even with these different implementations of 802.1x, there still are vulnerabilities with this method. 802.1x improved over WEP by: changing keys often eliminates the ability to discover keys; performing mutual authentication, it eliminates rogue Access Points from allowing "man in the middle" attacks; and authenticating users, it eliminates unauthorized usage (Riley 15). Using a VPN, IPSec, SSH, RADIUS, firewalls, etc. in

addition to one of these 802.1x implementations, can increase the level of security. Until 802.11i is fully released, there is no standard that dictates the way wireless security should be implemented, and 802.1x and EAP were not created with the additional risks of using a wireless network. They need to be reworked to include the special considerations that wireless usage introduces.

Virtual Private Networks (VPNs) are used to provide location transparency to remote users of a network and data security by sending data in an encrypted form (Khan and Khwaja 227). VPNs work with well with the wireless LAN security model, as they require authentication of users to use the VPN connectivity and cryptographic encryption algorithms for data. Internet Protocol Security (IPSec), is the most commonly used encryption protocol and Triple-Digital Encryption Standard (Triple-DES or 3-DES) is the most commonly used encryption algorithm (Khan and Khwaja 228). IPSec is an IETF standard for adding on security to traffic at the IP layer. VPN gateways, which facilitate the VPN connectivity between the remote site and the LAN, also act as DHCP servers and provide NAT services. There are software and hardware type VPN solutions, so they provide a flexibility that can work with any system. Plus, since the VPN idea is based on a standard that uses an encryption algorithm that has proven to be uncrackable, it is a good option for the wireless security world. VPNs can be added to the 802.1x/EAP setup to provide an even more secure solution.

Wi-Fi Protected Access (WPA)

The Wi-Fi Alliance, members including Microsoft, Cisco, Apple, Intel, have essentially lifted the 802.11i draft-in-progress to come out with an interim security solution for wireless, called Wi-Fi Protected Access (WPA) (Fleichman 1). This new pre-standard will abandon WEP entirely and move to Temporal Key Integrity Protocol (TKIP) for the encryption method. Additionally, the 802.1x port-based security idea will be included with this new security solution.

TKIP, sometimes referred to as WEP2, eliminates the problem in WEP of reuse of keys. "The TKIP process begins with a 128-bit "temporal key" shared among clients and access points. TKIP combines the temporal key with the client's MAC address and then adds a relatively large 16-octet initialization vector to produce the key that will encrypt the data. This procedure ensures that each station uses different key streams to encrypt the data" (Geier). TKIP still relies on the RC-4 encryption method, but has solved the WEP issues, but will be backwards compatible with the WEP systems. TKIP is a temporary solution as it is a software upgrade, until such time as hardware solutions based on the Advanced Encryption Standard (AES) comes to fruition (also part of the 802.11i draft). Jesse Walker of Intel discusses the four new algorithms added to WEP by using TKIP:

- Michael, a cryptographic message integrity code (MIC) to defeat forgeries.
- A new Initialization Vector (IV) sequencing discipline to remove replay attacks from the attacker's arsenal.
- A per-packet key mixing function, to take out the public IVs from weak keys.
- Finally, a rekeying mechanism, that eliminates the threat of attacks stemming from key reuse (Walker 2).

Other manufacturers have come out with TKIP type solutions to the wireless security problem. Symbol Technologies, for example, is utilizing a technology called Simple Secure Networks (SSNs), a encryption technology, that like TKIP, changes frequently (Edwards 1). This TKIP-type technology seems to be the agreed upon workaround to the WEP debacle.

“WPA contains the pieces of 802.11i that are closest to final approval, so few, if any, software changes should be required when 802.11i becomes "real" (Wexler “What’s in WPA”)

IEEE 802.11 Task Group I

As of yet, the 802.11i standard has not been ratified. The working group has basically completed the draft and is circulating it now to get final approval, with an expected release of September 2003. As previously mentioned, the WPA is based upon many of the proposed features of the 802.11i draft. These features are those that could be implemented at a relatively low cost, but still would be an improvement over WEP. Here is a list of the components that are shared by the WPA and by 802.11i: 802.1x authentication framework, access Point-to-client communications security, key hierarchy, key management, cipher and authentication negotiation, and Temporal Key Integrity Protocol, which rotates encryption keys on a per-packet basis and provides other important functions (Wexler, "What's In WPA?"). The IEEE sees TKIP is a short-term fix only to the WEP problem. Here are the components that will be included only in the 802.11i standard: AES, preauthentication (a strength when voice quality of service is required), peer-to-peer communications security (Wexler, "What's In WPA?"). Ultimately, a hardware fix is going to be required, and with that they are proposing using Advanced Encryption Standard (AES) as the encryption technology. The new hardware will require expensive changes in the manufacturing department, but may be backwards compatible with older technologies.

AES is an encryption standard now used in the government for sensitive, though unclassified information that has been approved as a Federal Information Processing Standard (FIPS). In 1997, the National Institute of Standards and Technology (NIST) had proposed the development of an unclassified, publicly disclosed and royalty-free

encryption algorithm to protect sensitive government information for now and into the next century ("Overview of the AES"). In 2000, Rijndael was chosen as the symmetric encryption algorithm to be part of AES and is an improvement over the DES algorithm. "The fact that the cipher and its inverse use different components practically eliminates the possibility for weak and semi-weak keys, as existing for DES" (Daemen & Rijmen 32). Rijndael was developed by two Belgian cryptographers in 1999 and beat out many other submissions as the algorithm of choice for AES to be based upon (Nechvatal, et al 1).

The Best Security Solution

The original 802.11 standard provided a wireless security solution that was innately flawed, partially because of the way the RC-4 cipher was implemented, and partially because of the lack of specifics about implementation written into the standard. Since that time, there have been many attempts to find a secure wireless solution. Which one is the best? In this case, "best" refers to: (1) least able to crack; (2) interoperable with other vendor equipment, so as not to limit someone to a specific vendor in this time of ever-changing corporate ownership; and (3) easy to set up. Though a level of security can be achieved, there seem to always be ways around every security measure. This is not to suggest that the "best" solution is completely without vulnerabilities.

WEP fell short of all three of these characteristics as: (1) the RC4 cipher that was implemented turned out to be easily crackable as the keys were reused too frequently; (2) the WEP specification did not provide enough specifics for vendors to make products interoperable, so though an Access Point may use WEP, the wireless card may use WEP in a different way; and (3) the WEP keys had to be manually set on all the Access Points and clients, so that changing them was a big chore.

The Cisco LEAP protocol seems to be close to achieving the goals of being the best wireless security solution. The Cisco hardware has been deployed into many locations, and LEAP has been applauded for the security it brings to the wireless world. Since Cisco has given its LEAP specification to other vendors, this has allowed less dependence on the Cisco hardware, but at this point, Cisco is not allowing other vendors

to build their own Access Points using the LEAP specification. This goes against the idea of getting away from proprietary technologies, so does not allow it to be the best wireless security option.

The other EAP-based 802.1x security solutions are also on the right track. They have been deployed in many areas. One is done by Microsoft and has been widely deployed, as it today is sold in many retail stores, for ease of access by everyone. Unfortunately, this product again runs into interoperability issues as using the Microsoft gear with other vendors' equipment, might not allow you to deploy the security measures.

I believe that the Symbol Technologies TKIP-like proposal is a good effort, but still not the best implementation idea for a corporation, simply because reliance on Symbol being in existence in a few years is not a sound decision.

Utilizing standards that allow for interoperability across the different vendors is a better way to go overall. Fortunately, the next generation, based on the WPA does include other vendors from the Wi-Fi consortium, so that there is no reliance on one vendors' proprietary technology. The WPA products are JUST shipping at this time, so they are untested in the real world for "uncrackability". This de facto standard is a step in the right direction and includes technologies used previously by Microsoft and Cisco and others, based on a known-good standard for port-based security, 802.1x. The use of RADIUS servers or Certificate Authorities is also important because these technologies

have been tested in the real world. The best advice sometimes is to use what is already known to work, and in this case, has been adapted to the uncertainties of wireless.

At this time, there is no “best” wireless security solution that meets the stated criteria. WEP is the only standard at the moment for 802.11 and no one seems to have faith in its ability to secure a network anymore. The recently released technologies look very promising and perhaps in six months the answer to this question may be different.

Conclusion

The future of wireless security looks a bit brighter with the ratification of the 802.11i standard on the horizon. As it is based upon a well-known standard of encryption, this provides hope that the implementation will be secure. Additionally, the IEEE should have learned from its mistakes with the WEP standard, so 802.11i should be a vast improvement. Unfortunately, the standards will need to keep evolving as hacks are found for each new security measure that is introduced.

Ultimately, the use of additional security measures, like adding VPN, RADIUS authentication, firewalls, physical security procedures, etc., makes wireless security safer. In studying information security in general, there are many common procedures to follow to make important data more secure. These measures can be used for wireless security as well. Security in general is a hot topic in every arena. There are common sense security measures that everyone can take to ensure a more secure environment (i.e. never tell someone your password or pin, always lock your computer screen when you step away, keep track of your laptop, secureIDs, etc.). These steps apply to wireless security as well.

The other wireless technologies, like Bluetooth and HomeRF are still out there and in use. They suffer from the similar security threats as the 802.11 standards. As the vendors work together to come up with de facto standards, this will help to find a secure way to implement these fascinating wireless technologies. Bluetooth is being widely watched for its variety of implementation uses. This makes developing security measures

all the more important, as Bluetooth's flourishing depends upon keeping up with the security 802.11 standards.

Unfortunately, it seems that there will always be attempts made to break any new encryption algorithm. As the new 802.11i standard is released, there may again be an effort to crack the new security technology. The Rijndael algorithm currently would require tremendous amounts of processor power to crack that are not easily or cheaply accessible today. But each year, the processor power seems to double in speed as the prices dramatically decrease. So in the not too distant future, this technology too may not be secure anymore.

"First you make it [security technology], then someone breaks it, then you fix it. And so on. There's never really an end point, " from a Wi-Fi spokesperson as quoted in Joanie Wexler's article "What's in WPA".

In the future, we may have biometric systems for authentication of every electronic device we use. Today, we have to practice the most secure methods of defense that are out there. We can do a the best job by using our brains and remembering to "Keep It Simple, Stupid."

Works Cited

Batista, Elisa. "FCC: HomeRF Gets Up to Speed." Wired News. 31 August 2000 <http://www.wired.com/news/print/0,1294,38564,00.html>.

Behr, Alyson, and Eric Butterfield. "Bluetooth: Still a Few Bumps in the Road." ZDNet UK Tech Update. 23 June 2002 <http://techupdate.zdnet.co.uk/story/0,,t481-s2112293,00.html>.

Borisov, Nikita, Ian Goldberg, and David Wagner. "Intercepting Mobile Communications: The Insecurity of 802.11" MOBICOM 2001 <http://www.cs.berkeley.edu/~daw/papers/wep-mob01.pdf>.

---. "Security of WEP Algorithm." <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>.

Brown, Bruce. "802.11a—Fast Wireless Networking". ExtremeTech. 3 December 2001 <http://www.extremetech.com/article2/0,3973,9151,00.asp>.

---. "Wireless Standards Up in the Air." ExtremeTech. 3 December 2001 <http://www.extremetech.com/article2/0,3973,9164,00.asp>.

Daemen, Joan, and Vincent Rijmen. AES Proposal: Rijndael. 9 March 1999 <http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael-ammended.pdf>.

Doshi, Nilesh. "Wireless LAN Security." Cisco Systems, Inc. Cisco Building L, San Jose. 28 February 2003.

Edwards, Mark Joseph. "Increasing Wireless Security with TKIP." Security Administrator. 23 October 2002 <http://www.secadministrator.com/Articles/Index.cfm?ArticleID=27064>.

"Extensible Authentication Protocol Transport Layer Security Deployment Guide for Wireless LAN Networks." Cisco Systems, Inc. White Paper. 13 November 2002. <http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/acstl_wp.htm>.

Fleishman, Glenn. "Key to Wi-Fi Security." InfoWorld. 10 January 2003 <http://www.infoworld.com/article/03/01/10/030113newifisec_1.html>.

Fluhrer, Scott, Itsik Mantin and Adi Shamir. "Weaknesses in the Key Scheduling Algorithm of RC4." Eighth Annual Workshop on Selected Areas in Cryptography. August 2001 <http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf>.

Franklin, Curt. "How Bluetooth Works." Marshall Brain's HowStuffWorks. < http://www.howstuffworks.com/bluetooth.htm>.

Gast, Matthew S. 802.11 Wireless Network: The Definitive Guide. Sebastopol: O'Reilly & Associates, Inc., 2002.

Geier, Jim. "802.1X Offers Authentication and Key Management." 802.11 Planet. 7 May 2002 <http://www.80211-planet.com/tutorials/article.php/1041171>.

Gordon, Matt. "TechWorks AirStation Wireless LAN." 27 April 2003 <http://www.hardwarecentral.com/hardwarecentral/reviews/2238/2/>.

IEEE."Port-Based Network Access Control." 802.1X <http://standards.ieee.org/getieee802/download/802.1X-2001.pdf>.

IETF. "PPP Extensible Authentication Protocol." RFC 2284. <http://www.ietf.org/rfc/rfc2284.txt>.

"Is This the End of Zombie HomeRF?" 802.11b Networking News. 25 April 2002 <http://80211b.weblogger.com/2002/04/25>.

Kaminiski, Chris. "Technology Overview of HomeRF 2.0". HomeNetHelp.com. 15 May 2001 <http://www.homenethelp.com/web/explain/about-homerf-2.asp >.

Khan, Jahanzeb, and Anis Khwaja. Building Secure Wireless Networks With 802.11. Indianapolis: Wiley Publishing, Inc., 2003.

Macnally, Cameron. "Cisco LEAP Protocol Description" . Online posting. 6 Sept. 2001 <http://lists.cistron.nl/pipermail/cistron-radius/2001-September/002042.html>.

Microsoft. "PEAP with MS-CHAP Version 2 for Secure Password-based Wireless Access." Microsoft TechNet by The Cable Guy. July 2002 <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/cableguy/cg0702.asp>.

Muller, Nathan J. Wireless A to Z. New York: McGraw-Hill, 2003.

Nechvatal, James, et al, comp. Report on the Development of the Advanced Encryption Standard (AES). United States. Department of Commerce. 2 October 2000 <http://csrc.nist.gov/CryptoToolkit/aes/round2/r2report.pdf>.

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

O'Hara, Bob, and Al Petrick. IEEE 802.11 Handbook: A Designer's Companion. New York: IEEE Press, 1999.

Potter, Bruce, and Bob Fleck. 802.11 Security. Sebastopol: O'Reilly & Associates, Inc., 2003.

"RC4 Encryption Algorithm" Online slide presentation. 5 March 2000 <http://www.ncat.edu/~grogans/main.htm>.

Riley, Steve. "Wireless LAN Security with 802.1x, EAP-TLS, and PEAP." MCS Trustworthy Computing Services. <http://www.blackhat.com/presentations/win-usa-03/bh-win-03-riley-wireless/bh-win-03-riley.pdf>.

Rivest, Ron. "RSA Security Response to Weaknesses in Key Scheduling Algorithm of

RC4." RSA Security. <http://www.rsasecurity.com/rsalabs/technotes/wep.html>.

Schenk, Rob, Andrew Garcia, and Russ Iwanchuk. "Wireless LAN Deployment and Security Basics." ExtremeTech. 29 August 2001 <http://www.extremetech.com/print_article/0,3998,a=13521,00.asp>.

Tyson, Jeff. "How Wireless Networking Works." Marshall Brain's HowStuffWorks. <http://www.howstuffworks.com/wireless-network.htm>.

United States. National Institute of Standards and Technology. "Overview of the AES Development Effort." February 2001 <http://csrc.nist.gov/CryptoToolkit/aes/index2.html>.

Walker, Jesse. 802.11 Security Series: Part II: The Temporal Key Integrity Protocol (TKIP). Intel Corporation. <http://cedar.intel.com/media/pdf/security/80211_part2.pdf>.

Wexler, Joanie. "Is Cisco LEAP-frogging the standards process?" NetworkWorldFusion. 5 March 2003 <http://www.nwfusion.com/newsletters/wireless/2003/0303wireless2.html>.

---. "What's In WPA?" NetworkWorldFusion. 13 November 2002 <http://www.nwfusion.com/newsletters/wireless/2002/01626699.html>.

Wireless Ethernet Compatibility Alliance (WECA). "802.11b Wired Equivalent Privacy (WEP) Security." 19 February 2001 <http://www.alvarion-usa.com/RunTime/Materials/KnowledgePoolFiles/C3_80211b_Wired_Equivalent_Privacy_Security.pdf>.