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 Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Wireless Security:
The Draft IEEE 802.11i Standard

Gregory D. Nowicki
GIAC Security Essentials Certification (GSEC)
5-May-2004

Abstract

Wireless technology has been a boon for both business and home users. Dependence upon this mode of connectivity carries a dark side. The aspect of sending your data into the air where there are no barriers to its propagation has provided another avenue for malicious users to gain access to your data and your network. In fact, one does not even need to have criminal intent to access another's wireless network. A large number of networks are setup with default network identification, no data encryption, and open access lists. Some client software is configured out of the box to connect to the first wireless network it finds. So without even being cognizant of it, your computer could be connected to your neighbor's set-up. This is the world of Wired Equivalency Protocol (WEP).

The IEEE standard that started it all, 802.11, was lacking in the area of security. In fact, it did not require any authentication or encryption. The standard did spell out an encryption method, but it was flawed in its design and did not provide any authentication. As a result, the original 802.11 committee formed a task group to remedy these problems. This was the ninth modification to the original standard, hence the group is known as TGi and its new standard is 802.11i. With a final draft almost completed, the wireless community can expect to start seeing 802.11i secured hardware on the market sometime this year.

This paper will attempt to give the reader some background on the existing problems with the current state of wireless security and what one can expect from the new standard currently under development. A bit of what is under the hood will be provided to reader while, hopefully, not becoming too bogged down in details. When referring to 802.11i in the rest of this paper, it is assumed to be the draft version unless otherwise noted.

Finally, it is concluded that the IEEE 802.11i standard being developed provides a quick fix in one form and offers more than one long-term solution for the wireless security problem.

WEP

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

In 1999, the IEEE produced the first wireless networking standard, 802.11. A full cryptographic analysis was never completed on the draft specification of its encryption mechanism and it used (arguably) the best cipher algorithm available at the time, RC4. The hardware produced under the standard sold very well, exceeding all expectations. With the burgeoning market for wireless products, flaws in its security implementation were quickly pointed out and in some cases, exploited. To understand these problems, a brief rundown on WEP is needed.

WEP provides the two most basic security necessities for a network packet: authentication and encryption. Authentication is provided by a 4-byte Integrity Check Value (ICV) that is appended to the packet. RC4 is a stream cipher which uses a 64-bit key. 24 of those bits are provided by an Initialization Vector (IV), the rest by a 40-bit shared key. Most vendor's implementations offer support for longer keys. The IV is generated by the sender using a method not specified by the standard. It can be changed periodically, but it is not mandatory. The entire data packet, including the ICV, is encrypted using the 64-bit (or longer) key by doing an exclusive OR (XOR) of the key and the packet. The key is reused as many times as needed to encrypt the whole packet. Decryption is just the opposite of encryption since if **x** XOR **y** produces **z**, then **z** XOR **y** produces **x**. In order for the receiver to be able to create the whole key using the IV and shared key, the IV must be contained in the packet in cleartext.

There are a good number of problems with WEP. Most of the major ones are listed below, but there are others aside from these and more found all the time.

1. Most wireless network equipment come with their security features, including WEP, turned off. The user has to make a conscious effort to enable it and then maintain a database of shared keys. These keys will need to be changed if they become public by way of equipment loss or employee attrition.
2. All of the keys are static; there is no way to dynamically change keys.
3. The IV is appended onto the packet in clear view. So an attacker knows part of the key just by looking at the packet.
4. It is possible to backout the key by looking for packets that were encrypted using the same IV and performing a statistical attack on the two cipertexts. As there are only 24-bits in the IV, a fully loaded AP with only one client can use all values in less than six hours. IV collisions will occur much more frequently when there is more than one client.
5. The WEP checksum (ICV) is based on a cyclic-redundancy-check (CRC-32) which is linear, thus providing an easy way to predict its behavior when examining two packets.

WAP and WAP2

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

In response to these problems, industry proposed and implemented WPA and WPA2. Both are backed by the Wi-Fi Alliance, but are not an IEEE standard. WPA (and WPA2) is a subset of the draft 802.11i standard that provides security for large enterprises and small office/home office WLANs. It consists of TKIP, CCMP, and authentication, basically everything in the 802.11i standard. It is designed to work with 802.11i, so it will be able to play with that equipment when devices are deployed which adhere to the final 802.11i standard. WPA2 uses AES instead of RC4 as its stream cipher. Several companies are currently shipping devices which conform to the specifications.

WPA and WPA2 close most of the holes found in WEP, but there has been no rigorous public examination of the implementation or algorithms. The Wi-Fi Alliance claims renowned cryptographers have examined the code, but it was done in a hurry without a large audience. This leads us to the central theme of this paper, 802.11i.

802.11i

The 802.11i standard is basically a wrapper around 802.11. It has three components which are spread into two layers. The lowest layer consists of two improved encryption algorithms; temporal key integrity protocol (TKIP) and the counter mode with CBC-MAC protocol (CCMP). On top of TKIP and CCMP sits 802.1x. Not actually a part of 802.11i, but another IEEE standard which provides port based access control and encryption key distribution. This standard will be explained further in the sections below.

TKIP

TKIP was designed to fix all the known problems and deficiencies in the WEP implementation and still be backward compatible with legacy devices. It was meant to be implemented as either a hardware or software upgrade to existing devices. There are three parts to TKIP, encryption, rekeying, and message integrity. At this time, devices meeting the 802.11i standard are not required to provide an implementation of TKIP.

Encryption still uses RC4, but with 128-bit keys. There is also an enhancement for the WEP IV problem. The IV is now 48-bits and is used as a sequence counter to prevent replay attacks. This allows fragmented packets which are received out of order to be dropped. There is now a two step per packet key mixing using the IV which breaks up the correlation used by weak key attacks. 2^48 packets can be exchanged before running out of unique IV allowing approximately 100 years of normal network traffic before key reuse occurs.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

There is one minor problem with RC4. It is a proprietary algorithm which has never been opened up to cryptographic analysis. Some years back, source code was released which is purported to be the algorithm and which produces the same results for all tests done so far. However it has never been claimed to be the 'real' RC4 by its inventor. This code does pass rigorous cryptographic analysis and the RC4 algorithm has never been found to be cryptographically compromised.

TKIP provides a rekeying mechanism allowing fresh integrity and encryption keys to be distributed. This mitigates some of the risk when using stale or weak keys.

Lastly, there is message integrity code (MIC), also called Michael, which provides a keyed cryptographic checksum of the packet. To create the checksum, the source and destination MAC addresses and the plaintext data of the packet are used. This guards against packet forgery attacks. Michael is not perfect. The MIC algorithm is targeted to provide at least 2^20 unique values even though it uses a 64-bit key. The best known attack using differential cryptanalysis can compromise the integrity check using about 2^29 messages.

CCMP

Along with the TKIP algorithm, the 802.11i standard defines another encryption method. Current hardware will most likely not be able to use this technique because of the additional overhead it places on the processor in most APs and STAs. This additional overhead is caused by the use of the advanced encryption standard (AES) as its cipher.

AES can be run in a variety of modes. CCMP uses counter mode with CBC-MAC (CCM). Encryption is provided by counter mode; authentication and packet integrity are provided for by CBC-MAC. AES is a symmetric block cipher which allows keys of various sizes. 802.11i calls for a key length of 128-bits. This particular mode of AES is designed for packet encryption only and has not been tested outside of that environment.

Other parts of the CCMP method include its own version of a MIC (not Michael) and a 48-bit IV called a packet number (PN). The CCMP algorithm is a required component of a valid 802.11i implementation.

AES is the latest encryption standard approved by the US Government for official use. It has no known weaknesses and withstood an extensive examination by well versed cryptographers. In addition to that, it beat out several other very fine algorithms in a head-to-head competition in order to become the official US encryption standard.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

WRAP

WRAP (Wireless Robust Authenticated Protocol) is another encryption protocol defined in the 802.11i standard. WRAP is based upon the Offset Codebook (OCB) mode of AES.

Three different parties have filed for patents on the WRAP algorithm. Because of this infighting, CCMP was introduced into the 802.11i standard as an optional component of the Robust Security Network (RSN) model. This paper will not explain this protocol further because it is possible that there will never be an option to use WRAP in any implementations of 802.11i. However, it is the long-term goal of the TGi committee that this be the de facto standard.

EAP

Extensible Authentication Protocol (EAP) was originally designed for point-to-point protocol (PPP), but it has been extended by 802.1x to handle all 802 networks. This is the authentication protocol that 802.1x uses to authorize a connection between a STA and AS. This layer is not the authentication method itself, but merely the transport for that method. This allows the changing of authentication methods without the AP having to be cognizant of that change.

This is the initial connection made between the AP and STA. All further communication between the STA and AP point depend upon the results that take place during this handshake. All methods requests by the STA are either authorized or rejected during this stage.

Since the authentication may take place over an unsecured network, 802.11x standard calls for using Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) over the link between the AP and STA. EAP-TLS allows for encrypted communication, thus protecting the message. Since this protocol is outside of the 802.11i standard, no further discussion of EAP-TLS will take place.

RSN

Robust Security Network (RSN) is the term applied to the strongest security model that 802.11i uses to authenticate, authorize, and protect the connection between the STA and AP. This is the combination of the most robust parts of the 802.11i standard: 802.1x for authentication and authorization, EAP for authentication transport, and support for stronger encryption algorithms such as AES. When there is a connection made between an AP and STA, that association is referred to as a Robust Security Network Association (RSNA).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Due to the overhead involved in implementing this mode, it is extremely unlikely that existing hardware will be able to provide this association. It is expected by TGi that all of the infrastructure hardware will be need to be upgraded mostly due to the load that the stronger encryption algorithms (only AES at this time) place on the AP and STA.

Keys

802.11i operates in two modes, pre-shared keys (PSK) or master keys exchanged with another component in the mix called an authentication server (AS). Most home and small-office networks will operate in the former mode. Larger networks can justify the cost of an AS, so they most likely will implement that option.

AS mode necessitates an initial authentication between the AS and the STA. This requires that the AP allow the STA to initially communicate with the AS. The two devices perform a handshake with the end result (hopefully) being that the STA has been authenticated and authorized to do something. The AS provides a primary master key (PMK) to both the AP and STA. That key contains information on the authorizations allowed to the STA. It then forgets that PMK, never to use it again.

PSK operates exactly as it does in WEP, but with better key creation and management. Master keys are still required to be shared with all of the systems on the wireless segment, but that key is only used to distribute fresh key material to both parties which then use that material to keep fresh keys on hand.

There are still some problems present with respect to keys. The fact that 802.11i still allows shared keys is a dilemma only solvable by forcing use of an AS. Key renegotiation when in a roaming environment is not fast enough to allow streaming data required by applications such as voice-over-IP. And then there is difficulty distributing broadcast/multicast keys which has not been fully resolved.

In conclusion:
WEP offers 40 or 104-bit RC4 encryption with a 24-bit wrapping IV. A CRC based data only integrity check and no key management.
TKIP provides 128-bit RC4 encryption with a 48-bit non-wrapping IV, Michael frame integrity check, IV based replay protection, and EAP based key management.
CCMP does TKIP better by offering 128-bit AES encryption and its own MIC.

802.1x

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

802.1x is a standard being developed outside of the 802.11i specification. Its primary tasks are authentication, authorization, and distribution of encryption keys. This standard is not tied to wireless and works equally well with dial-up or wired users. This provides support for a centralized security model. The primary encryption keys can be unique for each STA, reducing the traffic on any one key. When used with an AS, these keys can be generated dynamically reducing the amount of exposure of a particular key and providing reduced administrator configuration. The authentication model is not spelled out, thus providing support for future enhancements. At this time Remote Access Dial In User Service (RADIUS) RFC2865 is the de facto model.

The master key provided by 802.1x is only good until it expires or is revoked. This key is only used to distribute fresh keying material to both the AP and the STA and allow them to reestablish encrypted communication with each other during a reassociation.

Putting It All Together

A STA makes a request to access a network. As noted above, this can be either through a wireless or wired connection. The AP passes that request onto an AS which has authority to handle the particular request made by that STA. The two endpoints negotiate a master key (MK) which is actually a decision to allow the STA to access the requested service. Once authentication and authorization has been granted, pairwise master keys (PMK) are distributed to both the AP and STA. This set of keys spells out what authorization the STA is allowed. The PMK is then used to derive another set of keys called pairwise transient keys (PTK) which is a (large!) collection of operational keys:
1.) key confirmation key (KCK) – proves possession on the PMK by both parties.
2.) key encryption key (KEK) – encrypts the group transient key (GTK) which is used for multicast/broadcast traffic.
3.) temporal key (TK) – used for encrypting data traffic.
4.) Michael keys (64-bit, one for each end) when TKIP is being used.

Assuming that the all the keys are in place, communication can take place between the STA and AP. The packet header and data are signed using the appropriate MIC. This value is appended onto the end of the packet. The payload and MIC signature are then encrypted.

Encryption uses the TK provided by the above key exchange and the 48-bit IV. Once the IV has reached its maximum value and could possibly wrap, the 802.11i standard allows the communication to end or for a rekeying to take place.

Rekeying requires the use of the shared PMK to derive another set of operational keys. This is done pretty quickly, but the PMK is only good between a particular AP and STA. If the STA moves to another AP, it is required to undergo another

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

authentication with the associated AS. Using a shared key takes place of the PMK, thus providing authorization, authentication, and encryption.

Conclusions

The proposed 802.11i standard is a great leap forward in the wireless (and wired) environment. Even with the forced inclusion of the TKIP for legacy hardware, the vast majority of security problems present in the WEP standard have been mitigated. Granted, there are some security issues present such as a weak MIC (Michael) and the rekeying problem noted above, but the standard attempts to address all of them and work is currently ongoing to solve some of them before 802.11i is finalized.

Only time will tell as to how this standard will hold up in real life use. WEP was first thought to be a very secure algorithm, but now seemed plagued by every security bug there ever was. But the slow and deliberate proceedings of the IEEEs TGi is attempting to make sure as many security holes as possible are plugged before the standard is finished.

Now for the big question; what will be the name that marketing will give to this new technology?

Glossary

802.11 – First IEEE standard for wireless networks.
802.11i – Latest IEEE standard for WLAN confidentiality (draft status at this time)
802.1X – IEE standard for authentication.
AES – Advanced Encryption Standard: (Rijndael) a symmetric block cipher.
AP – Access Point: connection point between wireless and wired network segments.
AS – Authentication Server:
CCMP - Counter mode with CBC-MAC Protocol: an AES mode.
IEEE – Institute of Electrical and Electronics Engineers: an international society of engineers.
ICV – Integrity Check Value: WEPs CRC implementation for packets.
IV – Initialization Value: used to create a WEP key.
MAC – Media Access Control: physical address of the network device.
PEAP - Protected Extensible Authentication Protocol: WLAN authentication technology
RC4 – Encryption algorithm used in WEP, WPA, and (transitional) 802.11i. Developed by Ron Rivest.
RSN - Robust Security Network: most secure method described in 802.11i
RSNA - Robust Security Network Association

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

SSID - service set identifier: a 32 character network name used to connect to a specific AP.
STA – Station: Wireless client.
TKIP - Temporal Key Integrity Protocol: one of three encryption protocols spelled out in 802.11i.
ULA – Upper Layer Authentication: Authentication protocols above the MAC and physical layers.
WEP – Wired Equivalency Protocol (Wired Equivalent Privacy):
WLAN – Wireless Local Area Network
WPA – Wi-Fi Protected Access: A stopgap security measure between WEP and 802.11i.
WPA2 – Wi-Fi Protected Access V2: WPA with AES instead of RC4.
WRAP - Wireless Robust Authenticated Protocol: an encryption protocol in the 802.11i standard. Based upon the Offset Codebook (OCB) mode of AES.

References

1. 802.11 Security Series, Part II: The Temporal Key Integrity Protocol (TKIP), Jesse Walker. Technical report.

2. 802.11i standard:
http://standards.ieee.org/getieee802/download/802.1X-2001.pdf

3. Authentication and Authorization: The Big Picture with IEEE 802.1X, A Arthur Fisher, December 21, 2001
http://www.sans.org/rr/papers/6/123.pdf

4. Diving into the 802.11i Spec: A Tutorial, Dennis Eaton, Intersil, Nov 26, 2002:
http://www.commsdesign.com/design_center/wireless/design_corner/OEG20021126S0003

5. Examining 802.11i and WPA, The New Standards -- Up Close, By Frank Robinson, Apr 1, 2004:
http://www.nwc.com/story/singlePageFormat.jhtml;jsessionid=D1FSXHVCK5JBWQSNDBCCKHQ?articleID=18402840

6. IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines. P. Congdon, B. Aboba, A. Smith, G. Zorn, J. Roese. September 2003:
http://www.ietf.org/rfc/rfc3580.txt?number=3580

7. PPP Extensible Authentication Protocol (EAP). L. Blunk, J. Vollbrecht. March 1998:
http://www.ietf.org/rfc/rfc2284.txt?number=2284

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

8. Security of the WEP algorithm, Nikita Borisov, Ian Goldberg, and David Wagner
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

9. What is 802.11i?:
http://www.hackfaq.org/wireless-networks/802.11i.shtml

10. WEP (wired equivalent privacy):
http://www.nwfusion.com/details/715.html

© SANS Institute 2004, Author retains full rights.

Last Updated: July 25th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event