Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards

This paper describes the evolution of wireless security in 802.11 networks. The paper discusses the security weakness of Wired Equivalent Privacy (WEP) and provides with the interim and ultimate solutions: Wi-Fi Protected Access (WPA) and 802.11i standards. The paper begins with an introduction of WEP's well-known vulnerability, followed by the major requirements for securing wireless LANs. The paper then covers various responses from vendors, IEEE and the Wi-Fi Alliances. The Wi-Fi Alliances extracts the key features ...

Copyright SANS Institute
Author Retains Full Rights

AD

The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards

Stanley Wong

GSEC Practical v1.4b
May 20, 2003

Abstract

This paper describes the evolution of wireless security in 802.11 networks. The paper discusses the security weakness of Wired Equivalent Privacy (WEP) and provides with the interim and ultimate solutions: Wi-Fi Protected Access (WPA) and 802.11i standards.

The paper begins with an introduction of WEP's well-known vulnerability, followed by the major requirements for securing wireless LANs. The paper then covers various responses from vendors, IEEE and the Wi-Fi Alliances. The Wi-Fi Alliances extracts the key features from 802.11i to establish WPA to satisfy the immediate needs for the wireless industry. Meanwhile, IEEE 802.11 Task Group "I" is working on the 802.11i standard to provide the ultimate robust security for the wireless infrastructure. A high level of key features used by WPA and 802.11i, such as 801.X EAP based authentication, TKIP encryption protocol, AES encryption protocol, are explained. Summaries and potential issues of WPA and 802.11i are mentioned as well.

WEP Algorithm and its vulnerabilities

Wired Equivalent Privacy (WEP) was an encryption algorithm designed to provide wireless security for users implementing 802.11 wireless networks. WEP was developed by a group of volunteer IEEE members. The intention was to offer security through an 802.11 wireless network while the wireless data was transmitted from one end point to another over radio waves. WEP was used to protect wireless communication from eavesdropping (confidentiality), prevent unauthorized access to a wireless network (access control) and prevent tampering with transmitted messages (data integrity).

WEP uses the RC4 stream cipher, combining a 40-bit WEP key with a 24-bit random number known as an Initialization Vector (IV) to encrypt the data. The sender XORs the stream cipher with the actual data to produce ciphertext. The packet, combined with the IV with the ciphertext, is sent to the receiver. The receiver decrypts the packet using the stored WEP key and the attached IV[1].

[1] Borisov, Nikita. Goldberg, Ian. Wagner, David. "Security of the WEP algorithm". February 02, 2001. URL: http://www.isaac.cs.berkeley.edu/issac/wep-faq.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Unfortunately, the encryption protocol had not been subjected to a significant amount of peer review before release.[2] Serious security flaws were present in the protocol. Although the application of WEP may stop casual sniffers, experienced hackers can crack the WEP keys in a busy network within 15 minutes. In general, WEP was considered as a broken protocol.

The vulnerability of WEP can be attributed to the following:

1. WEP key recovery - WEP uses the same WEP key and a different IV to encrypt data. The IV has only a limited range (0 to 16777215) to choose from. Eventually, the same IVs may be used over and over again. By picking the repeating IVs out of the data stream, an attacker can ultimately have enough collection of data to crack the WEP key.

2. Unauthorized decryption and the violation of data integrity – Once the WEP key is revealed, a hacker may transform the ciphertext into its original form and understand the meaning of the data. Based on the understanding of the algorithm, a hacker may use the cracked WEP key to modify the ciphertext and forward the changed message to the receiver.

3. Poor key management – A proper WEP key is typed into a wireless device associated in a wireless network to enable the WEP. Unfortunately, there are no mechanisms to renew the stored WEP key. Once the WEP key is compromised, for example, an employee leaves a company; the key has to be changed in order to remain the security. The change of keys may be applicable in a home or small business environment. However, in an enterprise environment with thousands wireless mobile devices associated with the wireless network, the use of this method is almost impossible[3].

4. No access point authentication – WEP only provides a method for network interface cards (NICs) to authenticate access points. There is no way for access points to authenticate the NICs. As a result, it is possible for a hacker to reroute the data to access points through an alternate unauthorized path.

Custom solutions to WEP

Various vendors led the ways to produce their own solutions to address the weakness in WEP.

---

[2] Barnes, Douglas. "Network America: Wireless security? Read it and Wep". June 27, 2002. URL: http://www.vnunet.com/Features/1133066

[3] Dismukes, Trey "Azariah", "Ars Technica: Wireless Security Blackpaper". July 2002. URL: http://www.arstechnica.com/paedia/w/wireless/security-1.html .

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Enhanced WEP key – In 1998, Lucent pioneered a 128-bit WEP to extend the WEP key from 40-bit to 104-bit in order to enhance security. Under this approach, attackers might take longer amount of time to break the enhanced WEP keys. However, the approach was not very helpful because the previous security flaws in WEP still persisted. Agere and US Robotics also went after Lucent and created their own enhanced WEP solutions (Agere's 152-bit WEP and US Robotic's 256-bit WEP).

- Dynamic WEP key – Later, several vendors, including Cisco and Microsoft, implemented dynamic WEP re-keying of access points. The idea was to automatically generate short-lived, dynamic broadcast WEP keys at an interval set by a system administrator. The dynamic WEP keys prevented attackers from eavesdropping the communications. The attackers might never collect enough data to crack WEP keys.

- The implementation of VPNs – The wireless network can be further protected with the implementation of VPNs. Although VPN hardware may enable remote devices to establish a secure connection to access points, the VPN solution may fail to address seamless roaming when access points are crossed.

Some of these implementations may address the insecure issues inherent from WEP. However, the specific solutions from vendors may lead to poor interoperability in the long run.

Requirements for Secure Wireless LANs

The ultimate requirements of wireless security can fall into two categories[4]:

- Encryption and Data Privacy – The aim of encryption is to provide a mechanism to provide data privacy and integrity. The data should not be decrypted by any unauthorized means. All transmitted packets should be originated from the senders. The security mechanism should enforce the integrity of data under any circumstances.

- Authentication and Access Control – Authentication should be mutual, enabling wireless device clients and access points to authenticate each other. A framework should be introduced in order to facilitate the transmission of authentication messages between clients, access points and authentication servers. From the perspectives of access points, a mechanism should be introduced to validate client credentials in order to grant right level of access to the requested clients.

[4] Roshan, Pejman. "Securing Your Wireless LAN". 2001. URL: http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/esmnr_pg.pdf

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Responses from the 802.11 working group

In order to address WEP security issues, the 802.11 working group adopted the 802.1X standard for authentication, authorization and key management. At the same time, IEEE formed a Task Group "I" to develop 802.11i standard, with a purpose to produce a detailed specification to enhance the security features for wireless LANs dramatically.

The standardization of 802.11i is in process. Draft 3.0 of 802.11i is released in December 2002 and is currently in review. It is expected that the specification will be ratified by the end of 2003[5].

Industry Responses

The industry cannot wait for the 802.11i standard to be ratified by the end of 2003. It is demanding a more secure wireless environment in the present time. In response, the Wi-Fi Alliance, together with IEEE, develops the Wi-Fi Protected Access (WPA), an effort to address the WEP's vulnerability to offer a strong interoperable security standard to the market in the first quarter of 2003.

Wi-Fi Alliance

The Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of wireless local area network products based on IEEE 802.11 specification. Today, there are 183 member companies affiliated in the Wi-Fi Alliance. The Wi-Fi Alliance has certified 600+ Wi-Fi certified products. The goal of the Wi-Fi Alliance's member is to enhance the user experience through product interoperability[6].

Wi-Fi Protected Access (WPA)

The Wi-Fi Protected Access (WPA) is a standards-based interoperable security specification. The specification is designed so that only software or firmware upgrades are necessary for the existing or legacy hardware to meet the requirements. Its purpose is to increase the level of security for existing and future wireless LANs.

WPA is based on a subset of soon-to-be-finished 802.11i standard, including the following key features to address WEP vulnerabilities[7]:

---

[5] Gast, Matthew. "Wireless LAN Security: A Short History". April 19, 2002. URL: http://www.oreillynet.com/pub/a/wireless/2002/04/19/security.html
[6] Wi-Fi Alliance. "What is Wi-Fi?". URL: http://www.wi-fi.com/OpenSection/index.asp
[7] Wi-Fi Alliance. "Wi-Fi Protected Access – Overview". URL: http://www.wi-fi.com/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Implements 802.1X EAP based authentication to enforce mutual authentication
- Apply Temporal Key Integrity Protocol (TKIP) on existing RC4 WEP to impose strong data encryption
- Use Michael Message Integrity Check for message integrity

WPA is an interim security solution that targets on all known WEP vulnerabilities. It will be forward compatible with the upcoming 802.11i standard. The ultimate wireless security solution is still 802.11i. All products are supposed to comply with 802.11i standard once the standard is released.

WPA feature #1: 802.1X EAP based authentication

WPA adopts 802.1X to address the issue of user authentication in WEP. 802.1X initially is designed for wired networks but is also applicable to wireless networks. The standard provides port-based access control and mutual authentication between clients and access points via an authentication server.

802.1X standard is comprised of three elements[8].

- A supplicant – A user or a client wants to be authenticated. It can be the client software on a laptop, PDA or other wireless device.
- An authentication server – An authentication system, such as a RADIUS server, handles actual authentications.
- An authenticator – A device acts as an intermediary between a supplicant and an authentication server. Usually, the device is an access point.

The mutual authentication in 802.1X involves several steps:

1. A supplicant initiates a connection with an authenticator. The authenticator detects the initiation and enables the port of the supplicant. However, all the traffic except 802.11X ones, including DHCP, HTTP, FTP, SMTP and POP3, are blocked.
2. The authenticator then requests the identity from the supplicant.
3. The supplicant then responds with the identity. The authenticator passes the identity to an authentication server.
4. The authenticator server authenticates the identity of the supplicant. Once authenticated, an ACCEPT message is sent to the authenticator. The authenticator then transitions the supplicant's port to an authorized state.
5. The supplicant then requests the identity from the authentication server. The authentication server passes its identity to the supplicant
6. Once suppliant authenticates the identity of authentication server, all the traffics are forwarded thereafter.

[8] Snyder, Joel. "What is 802.1x?" May 06, 2002. URL: http://www.nwfusion.com/research/2002/0506whatisit.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The exact method of supplying identity is defined in the Extensible Authentication Protocol (EAP). EAP is the protocol that 802.1X uses to manage mutual authentication. The protocol provides a generalized framework for a wireless network system to choose a specific authentication method to authenticate. The authentication method can be passwords, PKI certificates or other authentication tokens. With a standardized EAP, an authenticator does not need to understand the details about authentication methods. The authenticator simply acts as a middleman to package and repackage EAP packets to pass from a supplicant to an authentication server, in which here an actual authentication will take place.

There are several types of EAP methods that are in use today.

1. EAP – LEAP
   This is a standard developed by Cisco. EAP-LEAP uses a username/password combination to transmit the identity to the RADIUS server for authentication.

2. EAP – TLS
   This is a standard outlined in RFC 2716. EAP-TLS uses a X.509 certificate to handle authentication.

3. EAP – TTLS
   This is a standard developed by Funk Software. EAP-TTLS is an alternative to EAP-TLS. While the authenticator identifies itself to the client with a server certificate, the supplicant uses a username/password identity instead.

4. EAP – PEAP (Protected EAP)
   Another standard designed to provide secure mutual authentication. The standard is designed to overcome some vulnerability that exists in other EAP methods.

There is a special case in 802.1X implementation. In the small users environment such as home or small business, an authentication server may not be available for authentication. As such, a pre-shared key mechanism is used. The shared key is placed to a supplicant and an authenticator manually. A similar WEP-like authentication is operated.

WPA feature #2: TKIP

Temporal Key Integrity Protocol (TKIP) is another element derived from 802.11i[9]. It is aimed to address WEP's known vulnerabilities in the area of data encryption. Specifically, TKIP fixes the security flaw of key reuse in WEP.

[9] Geier, Jim. "802.11 Security Beyond WEP". June 26, 2002. URL: http://www.80211-planet.com/tutorials/article.php/1377171

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

TKIP packet is comprised of three parts:

1. A 128-bit temporal key that is shared by both clients and access points.
2. An MAC address of a client device.
3. A 48-bit initialization vector describes a packet sequence number.

This combination guarantees various wireless clients use different keys.

In order to be compatible with existing hardware, TKIP uses the same encryption algorithm (RC4) as WEP. As such, only software or firmware upgrade is required to implement TKIP. Compared with WEP, TKIP changes the temporal keys every 10000 packets. This dynamic distribution leaves potential hackers little room to crack TKIP key.

In general, most security experts believe that TKIP is a stronger encryption than WEP. However, they also agree that TKIP should be an interim solution because of its use of RC4 algorithm.

WPA feature # 3: Michael Message Integrity Check

Michael Message Integrity Check is used to enforce data integrity. A Message Integrity Code (MIC) is a 64-bit message calculated using "Michael" algorithm[10]. Its aim is to detect potential packet content altercation due to transmission error or deliberate manipulation. The MIC is inserted in a TKIP packet.

A summary of WPA benefits

In general, the security advantages of WPA over WEP are:

- Apply stronger network access control through mutual authentication
- Support better security technologies like 802.1X, EAP, RADIUS and pre-shared keys
- Adopt dynamic keys in TKIP to establish better key management
- Enforce data integrity through Michael Message Integrity Check
- Provide forward compatibility to ultimate wireless security solution, 802.11i

However, WPA also presents some potential security issues:

- There are still potential encryption weaknesses in TKIP. Fortunately, the successful crack is expected to be heavy and expensive.
- Performance may be sacrificed potentially due to a more complex and computation intensive authentication and encryption protocols.

[10] Johnson, David. "Assorted 802.11 Related Crypto Algorithms". URL: http://www.deadhat.com/wlancrypto

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- The strength of WPA may still remain a uncertainty until further attack-proof.

802.11i: The ultimate wireless security solution

The 802.11i specification is a solution that IEEE 802.11 committee designs to target the security problems created by the WEP. The 802.11 Task Group "I" has been spending more than two years on the specification and three drafts have been released ever since. The 802.11i Task Group is getting closer to completion and the final release should be ready by the end of 2003.

The specification includes several key features:

- Encryption algorithms
  - TKIP - In order to support legacy device, the 802.11i chooses TKIP as one of the encryption standard (same as WPA).
  - CCMP – 802.11i also includes another standard known as AES-CCMP. AES stands for advanced encryption standard, which is a much stronger encryption algorithm that the US National Institutes of Standards and Technology (NIST) chose AES to replace the aging Data Encryption Standard (DES). However, AES-CCMP requires a hardware coprocessor to operate. Therefore, extra hardware is needed in the implementation of AES-CCMP.
  - WRAP - The last encryption that 802.11i includes is Wireless Robust Authentication Protocol (WRAP). Similar to CCMP, the encryption algorithm uses AES but another encryption mode (OCB) for encryption and integrity.
- Message Integrity – A strong data integrity algorithm (Michael Message Integrity Check) is applied (same as WPA).
- Mutual Authentication – 802.11i uses 802.1X/EAP for user authentication (same as WPA).
- Other security features - secure IBSS, secure fast handoff, and secure deauthentication and disassociation.
- Roaming Support

A summary of 802.11i benefits and potential issues

802.11i has all the advantages provided by WPA as mentioned above.

In additions, the 802.11i offers

- Stronger Encryption through the implementation of AES
- Roaming Support

The only issues of the 802.11i are:

- An extra requirement in hardware upgrade is required, in order to implement AES.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- A release is not ready until the end of 2003.

Conclusion

Wireless security has undergone major evolutions in last 7 years. WEP, the original security standard, is widely considered as broken. The IEEE 802.11 Group, the Wi-Fi Alliance and major network equipment vendors like Cisco are all working together to develop a new level of security standards.

WPA, an interim solution to the WEP vulnerability, is released in 2003. WPA, which uses a subset of 802.11i features, is generally believed as a major security improvement in wireless environment. WPA supports existing wireless infrastructure. Vendors can transit to the WPA standard through a software or firmware upgrade.

802.11i, the final solution to wireless security, is expected to provide the robust security required for wireless environment in the future. 802.11i is scheduled to be released by the end of 2003.

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

Barnes, Douglas. "Network America: Wireless security? Read it and Wep". June 27, 2002. URL: http://www.vnunet.com/Features/1133066

Borisov, Nikita. Goldberg, Ian. Wagner, David. "Security of the WEP algorithm". February 02, 2001. URL: http://www.isaac.cs.berkeley.edu/issac/wep-faq.html

Dismukes, Trey "Azariah", "Ars Technica: Wireless Security Blackpaper". July 2002. URL: http://www.arstechnica.com/paedia/w/wireless/security-1.html .

Gast, Matthew. "Wireless LAN Security: A Short History". April 19, 2002. URL: http://www.oreillynet.com/pub/a/wireless/2002/04/19/security.html

Geier, Jim. "802.11 Security Beyond WEP". June 26, 2002. URL: http://www.80211-planet.com/tutorials/article.php/1377171

Johnson, David. "Assorted 802.11 Related Crypto Algorithms". URL: http://www.deadhat.com/wlancrypto

Roshan, Pejman. "Securing Your Wireless LAN". 2001. URL: http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/esmnr_pg.pdf

Snyder, Joel. "What is 802.1x?" May 06, 2002. URL: http://www.nwfusion.com/research/2002/0506whatisit.html

Wi-Fi Alliance. "What is Wi-Fi?". URL: http://www.wi-fi.com/OpenSection/index.asp

Wi-Fi Alliance. "Wi-Fi Protected Access – Overview". URL: http://www.wi-fi.com/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**