A SURVEY OF WIRELESS NETWORK SECURITY PROTOCOLS

Jose Perez
Texas A&M University – Corpus Christi
Email: jluisperez16@gmail.com
Fax Number: (361) 825-2795
Faculty Advisor: Dr. Ahmed Mahdy, Texas A&M University – Corpus Christi

ABSTRACT

Today, the majority of wireless networks hold some form of sensitive data that only authorized users are meant to access. As a result, communication networks must enforce some type of security protocols that will limit the users who have access to the network resources. To ensure that a network is secure, the network must be able to enforce two key concepts: data privacy and data integrity. Data privacy is ensuring that all packets on the network are unreadable to any eavesdroppers while data integrity is ensuring that modified data is corrected. This paper discusses two of the most well known encryption protocols namely WEP and WPA/WPA2.

INTRODUCTION

To ensure that a network is secure, the network must be able to enforce two key concepts: data privacy and data integrity. Data privacy ensures that all packets on the network are unreadable to any eavesdroppers while data integrity ensures that modified data is corrected. Wired Equivalent Privacy (WEP) was the first wireless encryption protocol. As the name suggests, this protocol was designed to provide security analogous to that found on wire networks. In contrast to what its original intention was, WEP turned out to be rather insecure and susceptible to many outside attacks. Once WEP became a broken protocol, the Wi-Fi Alliance created WiFi Protected Access (WPA) and later, WPA2 that provides better security that is still unbroken.

WIRED EQUIVALENT PRIVACY (WEP)

WEP was introduced in IEEE’s original 802.11 standard in 1997 [15]. Standard 64-bit WEP consisted of a 24-bit initialization vector (IV) and a 40-bit key for data privacy [2]. To ensure that data has not been tampered en route, WEP uses a Cyclic Redundancy Check (CRC) value which is encrypted along with the packet load [10]. With both data privacy and data integrity in mind, WEP is a wireless encryption scheme that gives basic security for extremely small networks.

Encryption Process

While WEP uses a fixed IV length of 24-bits, the number of bits used for the key may range from 40-bits to a maximum of 104-bits [10]. Regardless of the number of bits used, encrypting a message goes through the same procedure. First, the Integrity Check Value (ICV) of the unencrypted message is determined via the CRC and appended to the end of the original message [10]. Afterwards, both the IV and key are passed into the Rivest Cipher 4 (RC4) algorithm to generate a key stream [10]. Once the key stream is generated, it is XORed with the original message to create the cipher text [10]. Upon completion, both the IV and cipher text are sent to the designated receiver. A visual representation of the previous process is presented below in Figure 1.

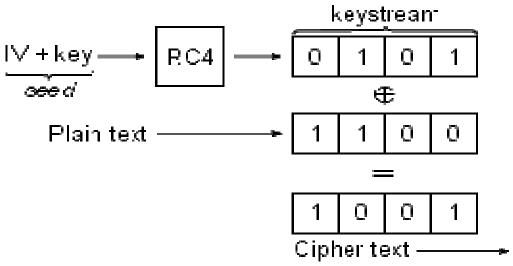

Fig. 1. WEP Encryption Process [14]

Decryption Process

Once a WEP encrypted packet is received at the end host, the entire encryption process occurs once again, but in reverse. First, the 24-bit IV and shared key are sent to the RC4 algorithm in an attempt to regenerate the same key stream used to originally encrypt the packet [10]. Once the key stream has been generated, the encrypted message and the key stream are XORed to decrypt all data in the encrypted packet [10]. From the decrypted packet, the ICV is checked from the data to ensure the data was not tampered with on delivery. If the data is not valid, the packet is dropped; otherwise, the message is determined to be authentic.

Authentication

WEP has two different authentication methods, Open System and Shared Key, which are used to determine which clients are allowed to gain access to the network's resources. In Open System Authentication, any client is allowed to join the network but this authentication stipulates that only those with the network key are allowed to send data [14]. While in Shared Key Authentication, only clients with the network key are allowed to join and gain access to the network's resources. Whenever the access point receives a request from a client, the access point sends the client a text challenge to encrypt to ensure that the client truly has the network key [14]. The client encrypts the text with its key and sends back the encrypted text to the access point for verification [14]. At the access point, the client's encrypted text is decrypted using the access point's key and compares with the text challenge, if both match, the client is allowed access to the network, if not, the client is denied access [14]. Figure 2 shows the Shared Key authentication process.

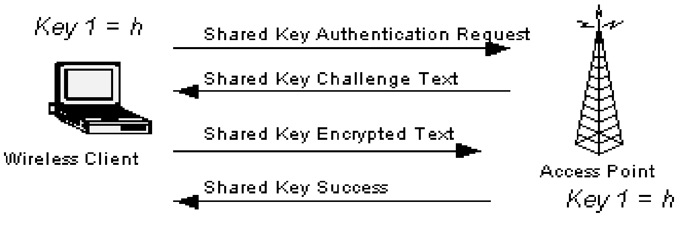
Key 1 = h
Shared Key Authentication Request
Shared Key Challenge Text
Shared Key Encrypted Text
Shared Key Success
Wireless Client
Access Point
Key 1 = h

Fig 2. Shared Key Authentication Process [6]

Weaknesses

Though WEP was quite useful in discouraging all but the most dedicated of malicious attackers, WEP had many flaws in its implementation that would lead to it being a broken algorithm.

i. IV Length Too Small

One weakness that WEP has is its small IV length of only 24-bits. With 24-bits, there is only 2^24 or 16,777,216 possibilities before a duplicate IV would be reused [5]. Such a small number of possibilities may be easily attainable on a busy network within a few hours [5]. Because of this, a malicious attacker would only need to generate all possible IVs in an attempt to decrypt any encrypted packets floating on the network [5].

ii. IVC Easily Modified

A network using WEP encryption may still accept tampered packets due to the way the IVC is calculated. Using CRC, the IVC is calculated linearly, meaning that if a malicious attacker were to change a bit in the message, they will only need to change the corresponding bit in IVC to make it appear genuine [2].

iii. Authentication Easily Bypassed

A network using WEP's Shared Key Authentication is very susceptible to eavesdropping. A malicious user only needs to collect both the encrypted text and the text challenge of a registered user connecting to the network [2, 5]. Once both the encrypted text and text challenge are collected, the malicious user would only need to use the XOR operation on them to discover the key to gain access to the network [5].

WI-FI PROTECTED ACCESS (WPA)

Once WEP was broken, millions of machines were virtually made unsecured overnight. With IEEE's 802.11i standard still in the drafting process, the Wi-Fi Alliance created WPA based on one of IEEE's drafts [4, 5]. One of the most notable weaknesses in WEP was the small key size; as such, WPA increased the IV to 48-bits and the key to 128-bits [1, 4, 5]. As a consequence of WEP's small IV which led to the reuse of keys, WPA uses the Temporal Key Integrity Protocol (TKIP) to manage keys and ensure no duplicates and weak keys are ever used [5]. To ensure that encrypted packets have not been tampered with, WPA uses *Michael* rather than the CRC that WEP uses [5].

Temporal Key Integrity Protocol (TKIP)

During the creation of WPA, the Wi-Fi Alliance saw the infeasibility of forcing millions of customers to purchase hardware upgrades to stay secure. As a result, TKIP was created to allow consumers to secure their networks through a firmware update rather than buying newer hardware [5]. In WPA, TKIP provides a complete key management system such as Master Key Creation, Temporal Key Derivation, and Duplicate Key Detection [5].

Michael

The Wi-Fi Alliance initially wanted to adopt an algorithm that used heavy multiplication to generate the message integrity check (MIC); but due to the low processing power of Wi-Fi cards, they settled on adopting *Michael* [5]. *Michael* was developed by Neils Ferguson in 2002 [5]. Rather then the heavy multiplication calculations that other data integrity algorithms use, Michael simply shifts and adds the bits [5].

Encryption Process

Since WPA was designed to improve on WEP, it is only sensible that the encryption/decryption process would be different. Before any packet may be encrypted, TKIP needs to have the temporal key that will be used to encrypt the packet, the MIC key used in *Michael* to calculate the MIC value, sequence counter, and the source address [4]. First, the temporal key, source address and the 32 most significant bits of the sequence counter are put into a key mixing algorithm which will yield a temporary key [4]. From there, the temporary key and the 16 least significant bits of the sequence counter are put into a second key mixing algorithm to yield the packet key [4]. Afterwards, the packet key is sent to the RC4 algorithm to generate a key stream that is XORed with the other data to yield the cipher text [13]. Figure 3 shows an overview of the WPA encryption process.

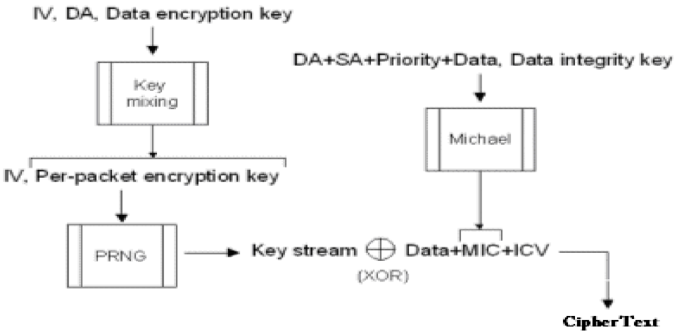
IV, DA, Data encryption key
Key mixing
DA+SA+Priority+Data, Data integrity key
Michael
IV, Per-packet encryption key
PRNG
Key stream
Data+MIC+ICV
(XOR)
CipherText

Fig. 3. WPA Encryption Process [13]

Decryption Process

Decryption of a WPA encrypted packet goes through essentially the same process but in reverse with numerous checkpoints to ensure the packet is valid [4]. First, TKIP must collect the same inputs as before to recover the seed used to encrypt the packet [4]. Afterwards, the sequence counter provided in the packet is checked to ensure that the packet has been received in order [4]. If the packet has yet to be received, the data, MIC, and ICV are decrypted. From there, *Michael* calculates the MIC of the packet and compares it with the MIC provided from the packet [4]. If *Michael* determines that both MICs are not the same, then counter measures are taken otherwise the packet is accepted [4].

Authentication

WPA was built to offer to types of authentication: Pre-Shared Key (PSK) and Enterprise. In WPA-PSK, any user wishing to access the network must provide this predetermined passphrase otherwise the connection would be refused by the AP. In contrast, authentication in WPA-Enterprise is provided by an IEEE 802.1x server rather than being handled by the AP [4, 11]. A user wishing to access the network must first request access to join the network from the AP [4, 11]. The AP then requests the client to send their identity and credentials [4, 11]. The client responds by sending them to the AP who forwards it to the authentication server [4, 11]. At the authentication server, the server validates the user's credentials and sends an accept or reject message to the AP [4, 11]. If the AP receives the reject message, then the client will not be able to access the network. Figure 5 shows the WPA- Enterprise authentication process.

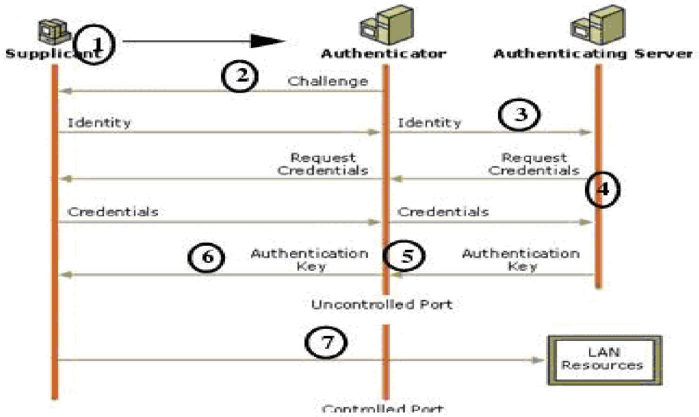

Fig. 5. WPA-Enterprise Authentication [11]

Weaknesses

While WPA was an attempt at securing networks that were left vulnerable by the cracking of WEP, WPA is also vulnerable to an extent.

i. Denial of Service (DoS)

WPA is very susceptible to DoS mainly because of the way it was built. Whenever a packet is received at the AP, *Michael* calculates the MIC of the data to ensure that it matches the one calculated at the source [4]. If *Michael* finds two packets that fail to match MICs within a span of one minute, it assumes that an attack is in progress and shuts down the network for one minute [4]. Any malicious user may use this safety measure to their advantage by constantly sending incorrect packets to the AP forcing *Michael* to shut the network down constantly.

ii. Simple Passphrases

Networks using WPA-PSK are also subject to Brute Force attacks unlike those using WPA-Enterprise mainly because of the form of authentication. WPA-PSK requires that a passphrase be predetermined to allow computers access to the network. If the passphrase is simple, a malicious user can perform a dictionary attack to gain access to the network.

CONCLUSION

Modern wireless communication networks are required to implement access control limiting access to authorized users and to ensure secure data transmission. In response, two wireless encryption protocols were created to secure such open networks from outside attackers and to keep their data secure; WEP and WPA/WPA2. This paper surveys the two protocols and discusses their relative strengths and weaknesses.

REFERENCES

1. Bohn, S., Brob, S., Nubgen, R., Schwann, P., An Automated System Interoperability Test Bed for WPA and WPA2, *2006 Radio and Wireless Symposium*, 615 – 618, 17-19 Jan. 2006.

2. Borse, M., Shinde, H., Wireless Security & Privacy, *2005 IEEE International Conference*, 424 – 428, 23-25 Jan. 2005.

3. Bragg, R., Rhodes - Ousley M., Strassberg, K., *Network Security: The Complete Reference*, Emeryville, California: McGraw-Hill, 2004.

4. Gast, Matthew S., *802.11 Wireless Networks: The Definitive Guide*, Sebastopol, CA: O'Reilly, 2005.

5. Edney, J., Arbaugh, W.A., *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*, Boston, MA: Pearson Education, Inc., 2005.

6. Extreme Tech, Wireless LAN Deployment and Security Basics, http://www.extremetech.com/article2/0,1697,1157726,00.asp, October 2007.

7. Filho E., Fonseca P., Leitao M., Barros P., Security versus Bandwidth: The Support of Mechanisms WEP e WPA in 802.11g Networks, *WOCN '07. IFIP International Conference*, 1 – 5, 2-4 July 2007.

8. Guyot, V., Using WEP in Ad-Hoc Networks, *2006 IFIP International Conference*, 4, 11-13 April 2006.

9. Gurkas G.Z., Zaim A.H., Aydin M.A., Security Mechanisms and their Performance Impacts on Wireless Local Area Networks, *2006 International Symposium*, 1 - 5, 16-18 June 2006.

10. Hassan, H.R., Challel, Y., Enhanced WEP: An Efficient Solution to WEP Threats, *Second IFIP International Conference*, 594 – 599, 6-8 March 2005.

11. Netgear, What are the Key Features of WPA Security?, http://documentation.netgear.com/reference/fra/wireless/WirelessNetworkingBasics-3-14.html, January 2008.

12. Netgear, What is WEP Encryption for Wireless Networks?, http://kbserver.netgear.com/kb_web_files/n100684.asp, October 2007.

13. The Cable Guy, Wi-Fi Protected Access Data Encryption and Integrity, http://technet.microsoft.com/en-us/library/bb878126.aspx, January 2008.

14. Wikipedia, Wired Equivalent Privacy, http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy, October 2007.

15. Wikipedia, Wi-Fi Protected Access, http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access, October 2007.