Improve Data Security through Firewall for Business Organization

Mrs. P.Anix Mary Javitha M.E. (CSE),
Computer Science and Engineering
St Joseph College of Engineering and Technology
Dar Es Salaam, Tanzania

***Abstract*- Firewall encryption services establish secure communication channels over the Internet assuring full privacy, authenticity and data integrity in corporate internetworking. Encryption helps to insure that the information within a session is not compromised. This includes not only reading the information within a data stream, but altering it, as well. While encryption has its own responsibilities in securing a communication session, maximum protection can be achieved. For this reason, many security protocols contain encryption specifications. In order to provide the good security for the data in a network, use WPA2-ENT (Wi-Fi protected access version 2 enterprise). This Enterprise method provides strong protection that works better in large business environments where users might frequently change.WPA2 -ENT creates new encryption keys each time users log on to the network with their unique passwords, and the passphrase to the network is not stored locally.**

I. INTRODUCTION

Firewalls can be used in a number of ways to add security to the business. Large corporations often have very complex firewalls in place to protect their extensive networks. On the outbound side, firewalls can be configured to prevent employees from sending certain types of emails or transmitting sensitive data outside of the network[2]. On the inbound side, firewalls can be programmed to prevent access to certain websites (like social networking sites). Additionally, firewalls can prevent outside computers from accessing computers inside the network. A company might choose to designate a single computer on the network for file sharing and all other computers could be restricted [1]. So a firewall is a good place to support strong user authentication as well as private or confidential communications between firewalls. Firewalls are an excellent place to focus security decisions and to enforce a network security policy. They are able to efficiently log internetwork activity, and limit the exposure of an organization. The exposure to attack is called the "zone of risk." If an organization is connected to the Internet without a firewall (Figure 1), every host on the private network can directly access any resource on the Internet. Or to put it as a security officer might, every host on the Internet can attack every host on the private network. Reducing the zone of risk is better. An internetwork firewall allows limiting the zone of risk.

The zone of risk becomes the firewall system itself (Figure 2). Now every host on the Internet can attack the firewall. In order to make the best choice for data security in network via firewall, need to select the suitable encryption protocols. Wired Equivalent Privacy (WEP) Protocol is a basic security feature, intended to provide confidentiality over a wireless network by encrypting information sent over the network [6].

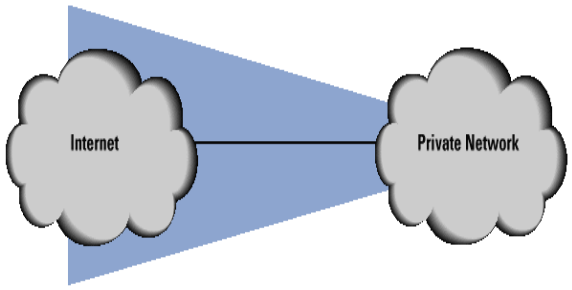

Figure 1 Zone of Risk for an Unprotected Private Network

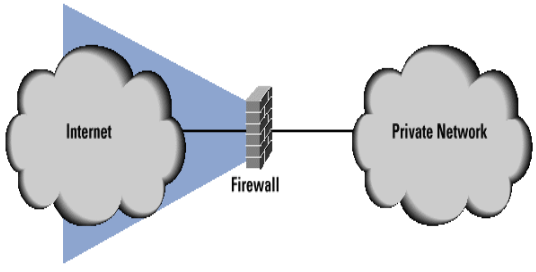

Figure 2 Zone of Risk with a Firewall

A. WEP and its vulnerabilities

A wireless network with data passing through WEP is susceptible to eavesdropping and data modification attacks (Figure 3). However, even when WEP is enabled, the confidentiality and integrity of wireless traffic is still at risk because a number of flaws in WEP have been revealed, which seriously undermine its claims to security. In particular, the following attacks on WEP are possible: (1) Passive attacks to decrypt traffic based on known plaintext and chosen cipher text attacks (2) Passive attacks to decrypt traffic based on statistical analysis on cipher texts (3) Active attacks to inject new traffic from unauthorized mobile stations (4) Active attacks to modify data; or (5) Active attacks to decrypt traffic, based on tricking the access point into redirecting wireless traffic to an attacker's machine.

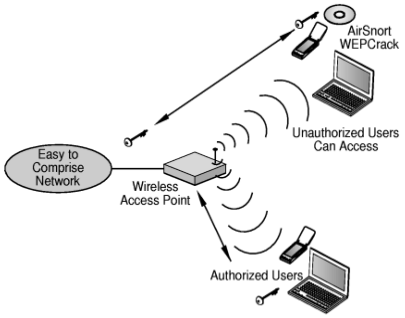

Figure 3. Unauthorized user access

A key-scheduling flaw has also been discovered in WEP, so it is now considered as unsecured because a WEP key can be cracked in a few minutes with the aid of automated tools. Even though many routers still include WEP, it's too insecure to rely on to protect the business. Instead, opt for one of the protocols in the WPA family.

B. WPA family

For secure wireless networks, the data encryption protocol is WPA, or Wi-Fi Protected Access. It is a wireless security protocol designed to address and fix the known security issues in WEP. WPA provides users with a higher level of assurance that their data will remain protected by using Temporal Key Integrity Protocol (TKIP) for data encryption. 8021x authentication has been introduced in this protocol to improve user authentication. Vulnerability in TKIP was uncovered where attacker may be able to decrypt small packets and inject arbitrary data into wireless network. Thus, TKIP encryption is no longer considered as a secure implementation. New deployments should consider using the stronger combination of WPA2 with AES encryption.

II. WPA2 WITH AES

Wi-Fi Protected Access 2 (WPA2), based on IEEE 802.11i, is a new wireless security protocol in which only authorized users can access a wireless device, with features supporting stronger cryptography (e.g. Advanced Encryption Standard or AES), stronger authentication control (e.g. Extensible Authentication Protocol or EAP), key management, replay attack protection and data integrity. The two WPA protocols are designed for different types of networks. WPA2-PSK is intended for home and very small office networks. Each wireless device is authenticated by the same 256-bit key. With this mode, set an encryption passphrase that must be entered by each user when connecting to the network. This passphrase can be stored on each computer, but it must be entered—or changed—individually for each device. All users share a locally stored passphrase, which can be found and copied from a computer by anyone. This makes WPA2-PSK less secure than the WPA2-ENT mode [8].

III. WPA2-ENT

WPA2-ENT is made for the enterprise network, but it's a smart choice for any business network. It provides security against more attacks than WPA2-PSK and separates users from the router's passphrase to the network. WPA2-ENT creates new encryption keys each time users log on to the network with their unique passwords, and the passphrase to the network is not stored locally. It also allows for centralized control over users' access to the wireless network, which makes management easier than with the WPA2-PSK mode.

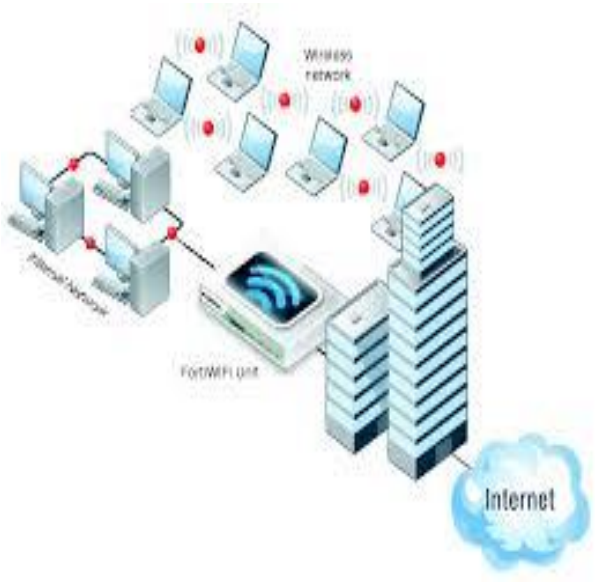

Figure 4. Network enterprise firewall

Users are assigned login credentials they must present when connecting to the network, which can be modified or revoked by administrators at anytime. Users never deal with the actual encryption keys. They are securely created and assigned per user session in the background after a user presents their login credentials. This prevents people from recovering the network key from computers.

A. WPA2 Authentication: Enterprise-level User Authentication via 802.1x/EAP and RADIUS

The authentication method used to verify the user (and server) credentials on WPA2-Enterprise networks is defined in the IEEE 802.1X standard. This requires an external server called a Remote Authentication Dial In User Service (RADIUS) [7]. A RADIUS server understands the Extensible Authentication Protocol (EAP) language and communicates with the wireless APs, referred to as RADIUS clients or authenticators. The RADIUS server basically serves as a middle-man between the APs and the user database. The AP is then communicate directly with the 802.1X client, also referred to as an 802.1X Supplicant, on the end-user's computer or device. Initial 802.1x communications begin with an unauthenticated supplicant (client device) attempting to connect with an authenticator (802.11 access point).

The client sends an EAP-start message. (1) This begins a series of message exchanges to authenticate the client (Figure 5). (2) The access point replies with an EAP-request identity message. (3) The client sends an EAP-response packet containing the identity to the authentication server. The access point responds by enabling a port for passing only EAP packets from the client to an authentication server located on the wired side of the access point. The access point blocks all other traffic, such as HTTP(Hyper Text Transfer Protocol) and POP3(Post Office Protocol3) packets, until the access point can verify the client's identity using an authentication server (for example, RADIUS). (4) The authentication server uses a specific authentication algorithm to verify the client's identity. This could be through the use of digital certificates or some other EAP authentication type. (5) The authentication server will either send an accept or reject message to the access point. (6) The access point sends an EAP-success packet (or reject packet) to the client. (7) If the authentication server accepts the client, then the access point will transmit the client's port to an authorized state and forward additional traffic.

802.1X authentication is port-based. This means that when someone attempts to connect to the enterprise-protected network, communication is allowed through a virtual port for the purpose of transferring login credentials. If authentication is successful, encryption keys are securely passed out and full access is given to the end-user [4]. Once the authentication process is complete the supplicant and authenticator have a secret MK (Master Key)

Figure 5. Client authentication [4]

B. Key generation in WPA2-ENT

WPA2 key generation is accomplished by means of two handshakes: a 4-Way Handshake for PTK (Pair-wise Transient Key) and GTK (Group Transient Key)

derivation, and a Group Key Handshake for GTK renewal [4][5]. The 4-Way Handshake, accomplished by four EAPoL (Extensible Authentication protocol over LAN)-Key messages between the client and the AP, is initiated by the access point and performs the following tasks: Confirm the client's knowledge of the PMK. The PMK derivation, required to generate the PTK, is dependent on the authentication method used. WPA2 Enterprise mode the PMK is derived from the authentication MK. Derive a fresh PTK, which is comprised of three types of keys: KCK (Key Confirmation Key – 128 bits) used to check the integrity of EAPoL-Key frames, KEK (Key Encryption Key – 128 bits) used to encrypt the GTK and the TK (Temporal Keys – 128 bits) used to secure data traffic. Install encryption and integrity keys. Encrypt transport of the GTK which is calculated by the AP from a random GMK (Group Master Key). Confirm the cipher suite selection.

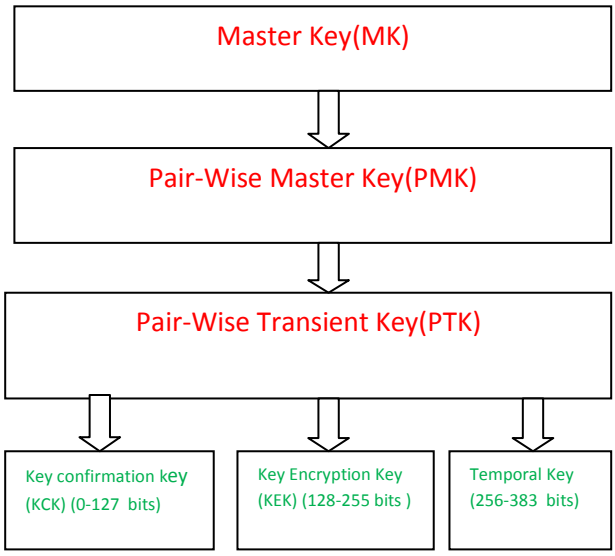

Figure 6. paie-wise Transient Key derivation

The Group Key Handshake is only used to disassociate a host or renew the GTK and uses the KEK generated during the 4-Way Handshake to encrypt the GTK.

C. *WPA2-ENT with AES*

AES is an extremely secure cryptographic algorithm with current analysis indicating that it takes 2^120 operations to break an AES key-a feat not yet accomplished. AES is a block cipher which is a type of symmetric key cipher that uses the same key for both encryption and decryption and uses groups of bits of fixed length-called blocks. Unlike WEP which uses a key stream acting across a plaintext data input stream for encryption, AES encrypts bits in blocks of plaintext that are independently calculated. The AES standard specifies an AES block size of 128 bits with three possible key lengths 128, 192 and 256 bits. A 128 bit key length is used for WPA2/802.11i. One round of WPA2/802.11i AES encryption is made up of four stages: [3] (1) substitute bytes (2) shift rows (3)Mix columns (4) Add Round key. With WPA2/802.11i, each round is iterated 10 times.

To provide both data confidentiality and authenticity, a new mode of construction called Counter-Mode/CBC-Mac (CCM) is used with AES. CCM employs AES in Counter mode (CTR) to achieve data confidentiality and AES using Cipher Block Chaining Message Authentication Code (CBC-MAC) to provide data integrity. CBC-MAC is used to generate an authentication component as a result of the encryption process . This is different from prior Message Integrity Code (MIC) implementations, in which a separate algorithm for integrity check is required. To further enhance its advanced encryption capabilities, AES uses a 128-bit Initialization Vector (IV).

IV. WPA2 ENCRYPTION STEPS

The MIC-similar to a checksum - provides data integrity for the non-changeable fields in the 802.11 header, unlike WEP and WPA, preventing packet replay from being exploited to decrypt the package or compromise cryptographic information.

A. *CBC-MAC Mode Algorithm*

The MIC is calculated using a 128-bit IV as follows (Figure 7): MIC =Pi XOR E(TK,IV) [3] (1) IV is encrypted with AES and TK to produce a 128-bit result. (2). 128-bit result is XOR with the next 128 bits of data. (3). The result of XOR is then passed through steps 1 and 2 until all 128 blocks in the 802.11 payload are exhausted. (4). At the end of the operation the first 64 bits are used to produce the MIC.

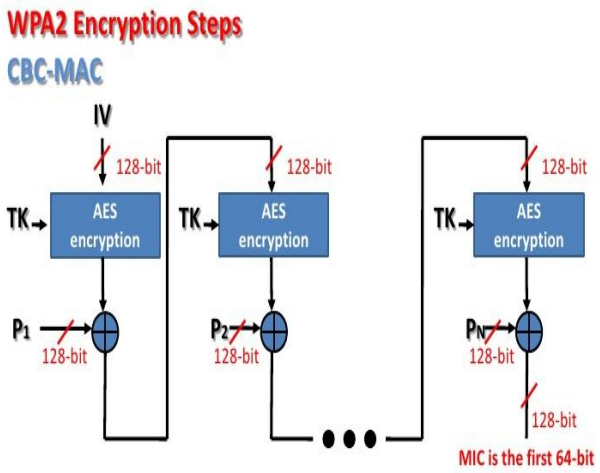

Figure 7. CBC-MAC mode in encryption[4]

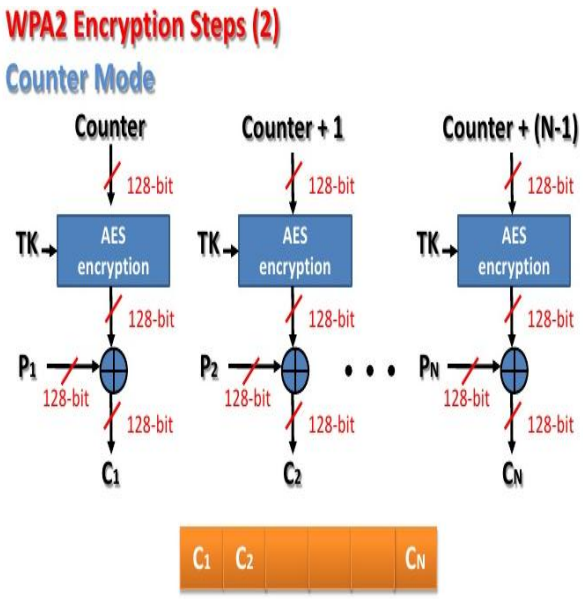

Figure 8(a). Counter mode for encryption[4]

B. Counter Mode Algorithm

The Counter Mode algorithm encrypts the data and the MIC (calculated using the CBC-MAC). The Counter Mode algorithm begins with a 128-bit counter preload similar to the MIC IV, but uses a counter value initialized to 1 instead of a data length resulting in a different counter used to encrypt each packet. The data and the MIC are encrypted as follows (Figure8(a)): (1) Initialize counter if it is the first time otherwise increment counter.(2).

First 128 bits are encrypted using AES and TK to produce a 128-bit result. (3). A XOR is performed on the result of step 1. (4) The first 128 bits of data produce the first 128-bit encrypted block. (5). Repeat steps 1-4 until all the 128-bit blocks have been encrypted. (6). Set counter to zero and encrypt it using AES and XOR with MIC appending the result the encrypted frame (Figure 8(b)).

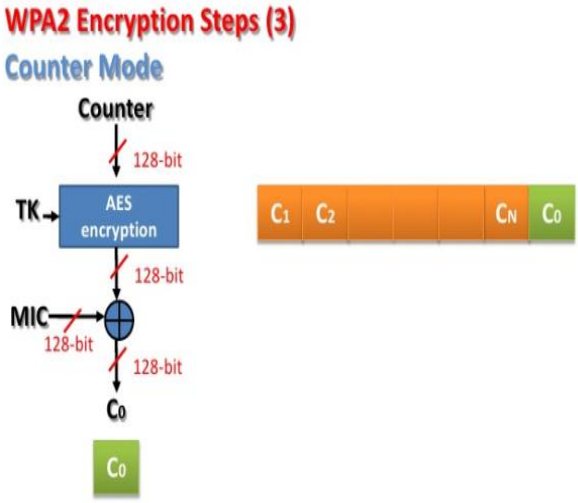

Figure 8(b). Cipher Text Generation[4]

V. WPA2 DECRYPTION STEPS

Decryption works in reverse. Here are the summarized steps [5]: (1). Using the same algorithm for encryption the counter value is derived. (2). The value from step 1 and the encrypted portion of the 802.11 payload are decrypted using the Counter Mode algorithm and TK. The result is the MIC (Figure 9(a), 9(b)) and decrypted data. (3). The date then is processed by the

CBC-MAC algorithm to recalculate the MIC (Figure 10) and the values from step 3 and 2 do not match the packet is dropped. Otherwise, the decrypted data is sent up to the network stack and to the client.

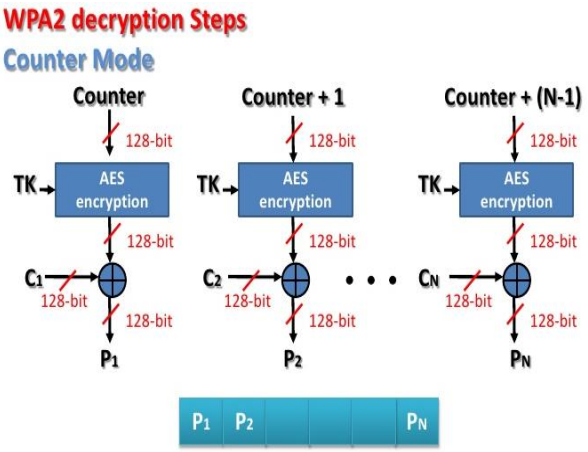

Figure 9(a). Counter Mode For Decryption[4]

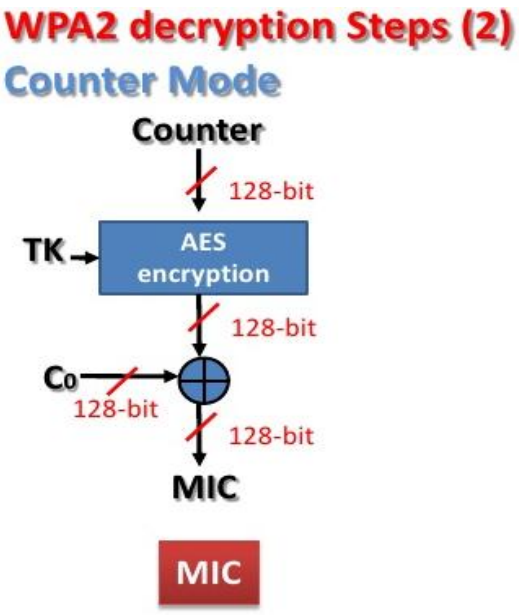

Figure 9(b). counter mode for MIC decryption[4]

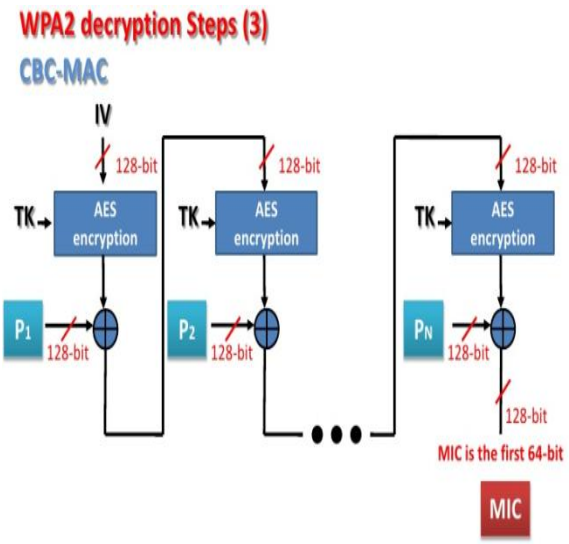

Figure 10. CBC-MAC mode for decryption[4]

VI. CONCLUSION

The organization should develop a strong wireless security policy to address all the usage options of wireless networks and the types of information that can be transmitted. While Wi-Fi security is more than an encryption choice, choosing the wrong protocol can leave the network vulnerable to attack. Wi-Fi technology evolves with time, and WPA2-ENT has been considered the most secure method of protecting Wi-Fi connection in business environment. While there are other methods of Wi-Fi encryption, WPA2-ENT is recommended for wireless security [9].

In encryption benefits, WPA2 adds two enhancements to support fast roaming of wireless clients moving between wireless AP's. PMK caching support – allows for reconnections to AP's that the client has recently been connected without the need to re-authenticate. Pre-authentication support – allows a client to pre-authenticate with an AP towards which it is moving while still maintaining a connection to the AP it's moving away from. PMK caching support and Pre-authentication support enable WPA2 to reduce the roaming time from over a second to less than 1/10th of a second. The ultimate benefit of the fast roaming is that WPA2 can now support timing-sensitive applications like Citrix,

REFERENCES

[1]. Richard E . Smith, 2004 internet cryptography, Low price edition

[2]. Basics of network security, firewall and VPN, 2003, NIIT

[3]. William Stallings, 2009, cryptography and network Security- principles and practices, fourth edition, LPE

[4]. Wifiprotected access 2, published bymshari AlabdulKARIM, http://www.slideshare.net/ENGMSHARI/wpa2

[5]. Benefits and vulnerabilities if wifiprotecd acees 2 by paul arana infs612-fall 2006 Wi-Fi Protected Access - Wikipedia,the Free encyclopedia *en.wikipedia.org/wiki/Wi Fi_Protected _Access*

[6].Wireless networking basics, may 2005, documentation.netgear.com*/wpn802/enu/202.../WPN802-09-17.html*

[7].http://www.ezlan.net/wpa_wep.html,Wireless Encryption - WEP, WPA, and WPA2

[8]. Bulk, Frank. "Learn the basics of WPA2 Wi-Fi security". Network Computing Jan. 27 2006. http://www.informationweek.com/story/showArticle.jhtml?articleID=177105338

[9]. Cisco Wireless LAN Security Overview http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps430/ps4076/prod_brochure09186a00801f7d0b.html