LAMK Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

WIRELESS NETWORK SECURITY

A GUIDE FOR SMALL AND MEDIUM PREMISES

LAHTI UNIVERSITY OF APPLIED SCIENCES
Degree programme in Business Information Technology
Bachelor’s Thesis
Spring 2018
Hoa Gia Bao Nguyen

Lahti University of Applied Sciences
Degree Programme in Business Information Technology

Nguyen, Hoa Gia Bao

Title: Wireless Network Security – A Guild for Small and Medium Premises

Bachelor's Thesis in Business Information Technology

49 pages

Spring 2018

ABSTRACT

The 21th Century is defined by human scientific breakthroughs. One of them is the global use of the Internet. Almost every educated person nowadays knows more or less about the internet. Thereby, a large percentage of the human population make use of the internet on a daily basis. Wireless internet access is thereby made affordable and accessible for everyone and that has boosted human communication and economy development into a new era. However, along with benefits, wireless internet access also possesses several risks and threats of security. The Internet has become a fertile land for criminals of all kinds to operate. Most of the time what they try to take is personal information, some of them of extreme values and sensitivity, from naive and unaware users. In that sense, a comprehensive study on how cybercriminal carry out their attacks and how to avoid and actually prevent such attacks if possible would be beneficial for the righteous netizens.

Keywords: Wireless, WLAN, Security, Internet, Protection, Cyber threats, Access, Information Technology, Computer Science.

Table of Contents

Table of Figures

Glossary

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
AP	Access Point
CRC32	Cyclic Redundancy Check 32
EAP	Extensible Authentication Protocol
EAS	Enterprise Access Server
ECB	Electronic Code Block
ICV	Integrity Check Value
IV	Initialization Vector
MAC	Media Access Control
OTP	One-time Password
PC	Personal Computer
MCIA	Memory Card International Association
PPTP	Point-to-Point Tunneling Protocol
RADIUS	Remote Authentication Dial-in User Service
RC4	Rivest Cipher 4
SSID	Service Set Identifier
SSL	Secure Socket Layer
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

1 RESEARCH FRAMEWORK

1.1 Research method

Research methods are planning, executing protocols and algorithms to reach and satisfy the research purposes. Researchers can determine a clear and detailed plan for their studies and a solution for their research motivations or problems. There are usually two main research methods: Deductive and Inductive.

Deductive: Deductive method is by going through already proven data and previous theories. The researchers they're by filter and reprocess such data and theories and apply such processes information into their own research cases and come up with their own solutions and conclusions (Walliman, 2011).

Inductive: The researchers start with a new theory and then will observe and test that hypothesis to prove and confirm that theory. Going from a more general viewpoint to a smaller specific target (Nayak & Singh, 2015).

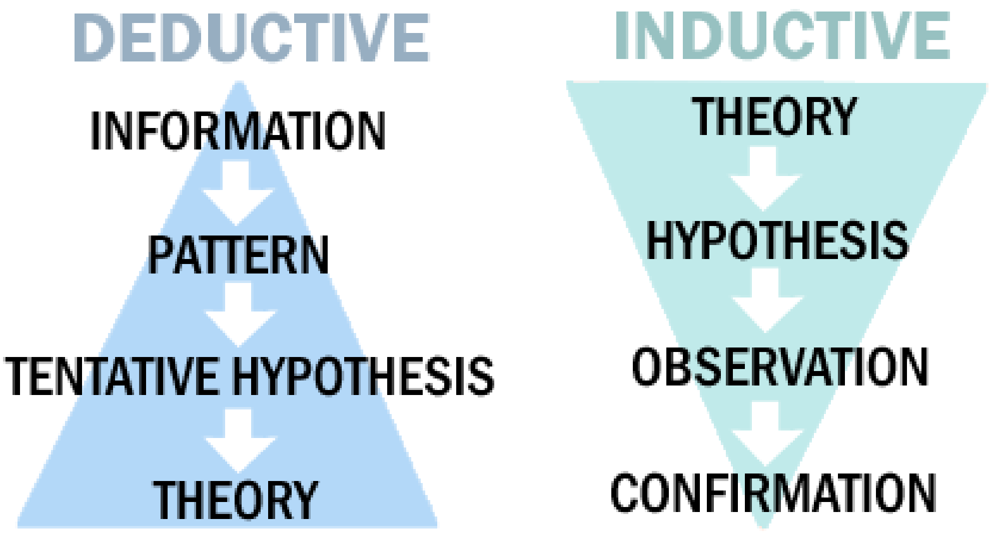


Image 1: Comparison between Deductive method and Inductive method

Considering the research question and the abundance of information and studies on the topic, it would not be more productive if the thesis author tries to do more innovative researches and try to come up with new approaches or theories. Instead, the thesis author could make use of the already numerous and specific study and approaches on the same matter and apply them into his own specific case. Therefore, the thesis will obviously follow the deductive research approach. This approach ensure that previous valuable information is made use of in the most efficient manner and that the author does not go on a wide goose chase trying to come up with solutions that do not guarantee better worth end values.

1.2 Research motivation

Nowadays, almost every business is setting free Wi-Fi hotspots as a complementary service for customers and visitors. Such a move not only provide a more comfortable and convenient environment for the customer but also helps boost the favour attitude of the customers towards the business. Those businesses that adopt this practice are those that are frequented by a large number of people such as coffee shops, shopping malls, restaurants, hotels as well as public premises such as airports, harbours…

Due to the privacy right for the customers and visitors, business owners and security forces cannot go around and physically check what their customers are doing with the free connection they currently have. That fact poses great risks and threats towards both the system of the premise and other unwary users. Attack method comes in various methods, forms and scales as well as damaging consequences. Some result in temporary or permanent downfall of the WLAN network. Other steal sensitive information such as biological data and financial activities or social media passwords and access.

Still, free Wi-Fi services are so effective and profitable to business owners as they are convenient to customers that abolishing them all together is entirely not an option. Thus, business owners must figure out different methods of counter-striking attacks on their networks to ensure data safety. For such as mission to be possible, a thorough understanding of what a WLAN network is made of and how cyber criminals can find their way pass the security measures and what could be done to prevent such attacks from happening is a must. However, most of the time, those owners are business men with knowledge in business management, marketing, financial accounting and other business-related skills. Commonly, they lack the very basic knowledges of how to understand and configure their own WLAN networks, much less protecting them from attack from cyber criminals who had spent their entire life horning technical skills and knowledge.

In this study, the thesis author will present the detail about the above-mentioned issues in a clear and scientific manner so that such knowledge can be comprehended by business and public premise owners.

1.3 Research question

Since this thesis will concern the study and application of Internet Technologies and Security Measures that can be uses and understood by small-size and medium-sized public businesses and premises, the following research will act as the main concern and thus the research question.

"What do small-size and medium-size public businesses and premises need to know about WLAN connection and WLAN security on a technical and practical manner?"

1.4 Thesis structure

Generally, the research papers contain eight chapters. In chapter one, the thesis author states his research framework such as research methods, research motivation and research question. Chapter two is about the introduction of the WLAN network, its definition, structure, advantages and disadvantages. Forwarding on, chapter three continues to Wireless security and components of a WLAN client.

Next, chapter four provides information about cryptography and encryptions, types and methods. Chapter five focuses on more about WEP (Wired Equivalent Privacy) a protection that secures information while it is in transmit. Chapter six will list out today’s common cyber attacking methods to the WLAN network.

Continues to chapter seven will answering the research question that was stated in chapter one. Chapter eight will be the discussion about the thesis’s limitations, validity, reliability and the summarize of the whole research paper.

2 INTRODUCTIONS TO WIRELESS LAN

2.1 Definition

A wireless network is a network of devices such as computers, printers, mobile devices that could communicate and share information with each other via wireless internet connection better knowns as "wi-fi”. A wireless network makes no use of cables of any kind. Such is possible by the use of access point devices (for Wi-Fi routers), wireless card (for Pcs), PCMCIA (for laptops without built-in wifi access components) (Bing, 2000).

A wireless network can either be an indoor or an outdoor network as illustrated below in image 2 and image 3.

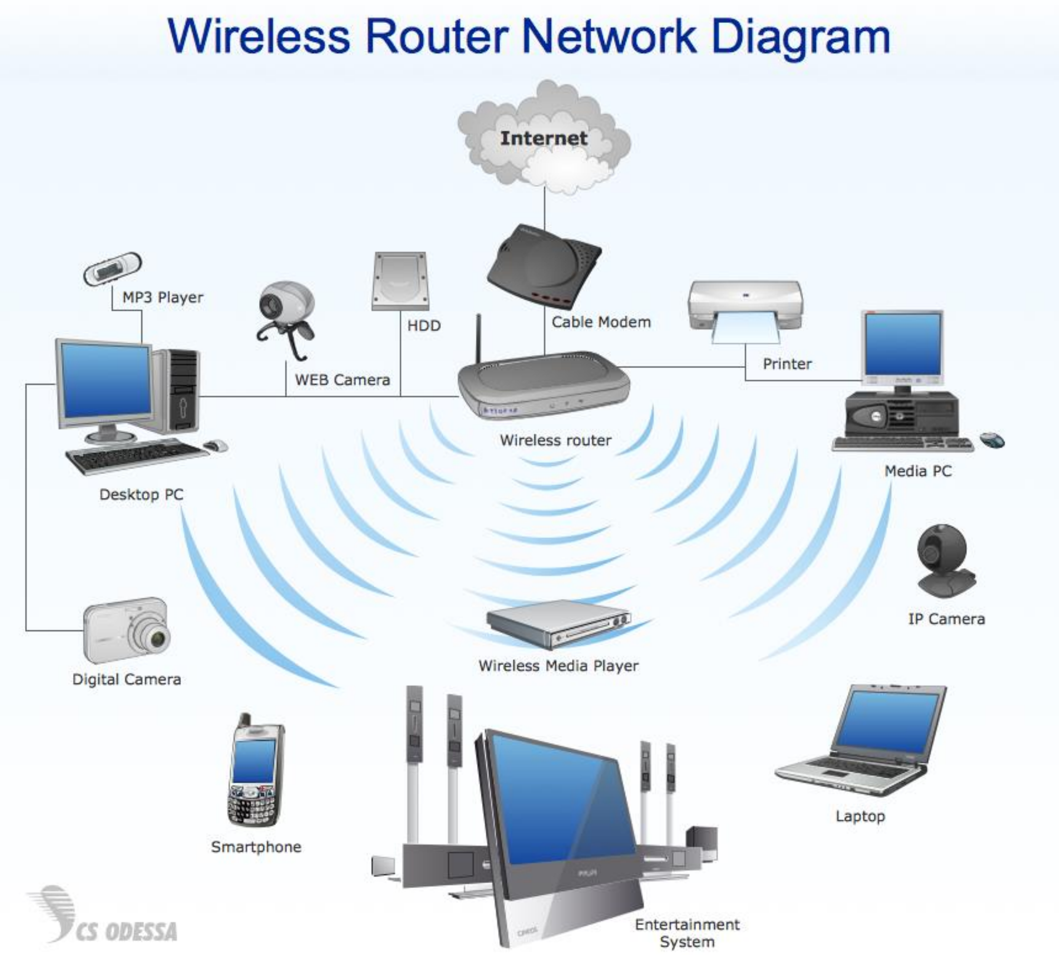


Image 2: An indoor wireless network diagram

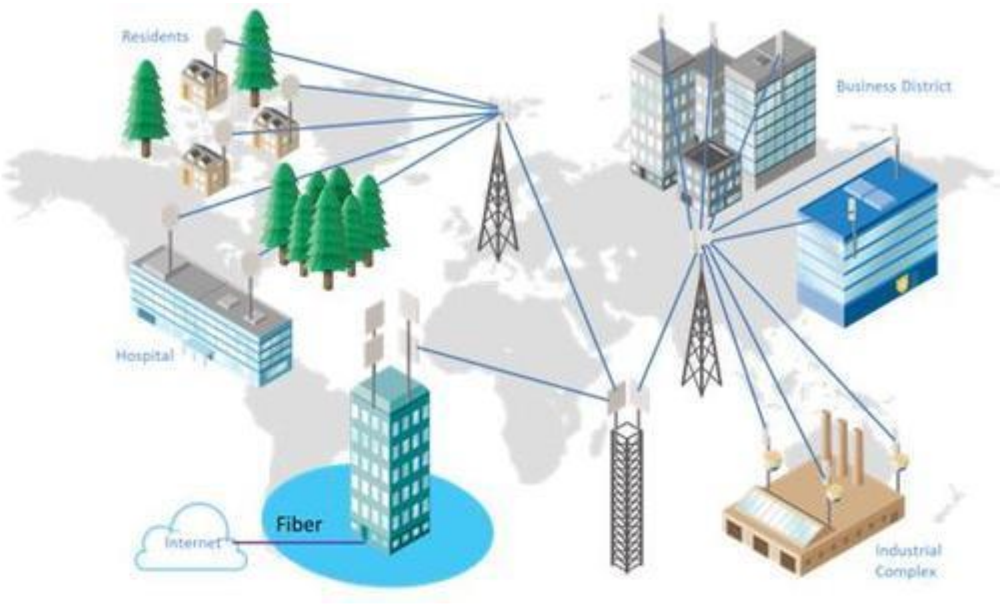


Image 3: An outdoor wireless network diagram

2.2 Advantages

As said above, a wireless network makes no use of cables for connection but uses radio frequency. The greatest advantage of a wireless network is mobility. Users are not limited by space and access points.

- Mobility

Users of wifi-enabled devices such as laptops, notebooks or smart devices can move around often and still retain stable connection speed. This allows those users to move around, for example, in conferences, cafes, classrooms and libraries and still not lose online access. Without a wireless connection, users are bound to a location reachable by internet cable (Bing, 2000).

- Cost-effective on the long run

Initial investment for a wireless connection, while varying from country to country and depending on specific service providers and contract terms, is generally affordable for most people and such connection can be used over the course of a few years. A cable-enabled connection may cost more due to extended material cost and maintenance fees for connection devices. In addition, a wireless network is effective in environments where mobility is a must which could have never been achieve by traditional cable-enabled network (Harte, 2004).

- Easy to connect in public areas

Nowadays, a public connection to the internet is considered a basic necessity in the human society. In public properties frequented by hundreds or even thousands of people such as airports, government buildings and economic businesses, a wireless network is the most viable option to allow access to the internet. Wireless connection helps people navigate better and work uninterrupted and thus help improve the properties' favours and reputation as well as visitor rates and economic development (Gary, 2016).

2.3 Structure

An 802.11 wireless network is varied in its structural components. However, it can be classified according to 3 main models.

- IBSSs - also knowns as Ad Hoc wireless
- BSSs - also knowns as Infrastructure wireless
- ESSs - also knowns as Extended Mesh wireless

Sometimes referred to as Peer-to-Peer WLANs, the AD HOC model only requires that client radios are connected to the network. There is no access point or network overseer, and each workstation must be close to each other and the data broadcasted from one workstation is transferred directly to the receiver station. This type of network is commonly used when a user wants to set up a WLAN network among different laptops in a conference setting or when there is no access point for users to connect and share information (Bing, 2001).

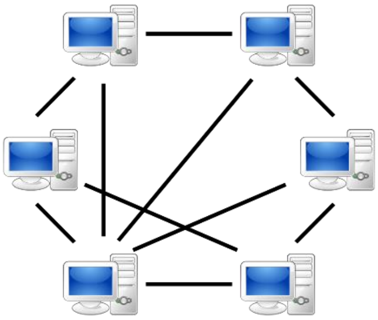


Image 4: An AD-HOC WLAN structure

The below image illustrates the infrastructure wireless network model:

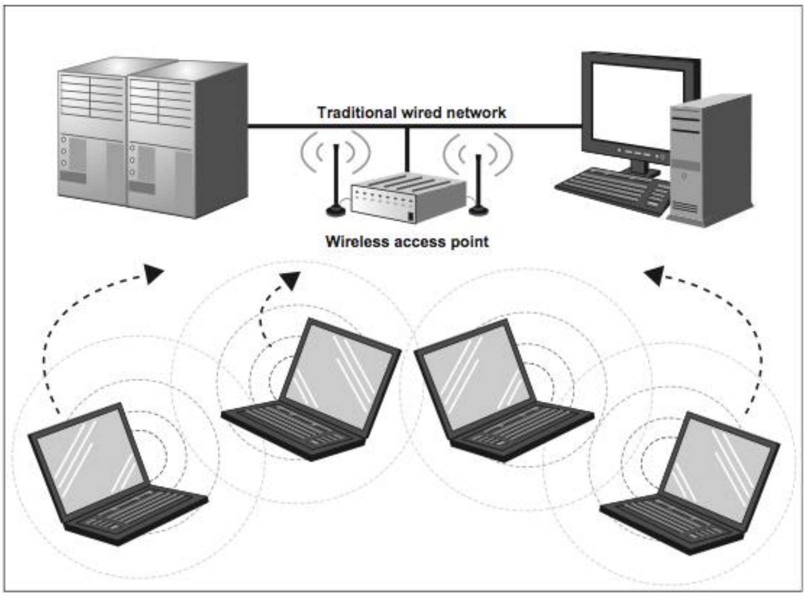


Image 5: A BSSs wireless Structure

This type of model includes one or several access points that are connected to the internet (such as wifi routers) and several client workstations. The client workstations connect to the internet via an access point. Individual client workstation does not communicate directly to each other but rather to platforms and protocols in the internet (via the access point). Each access point can support a certain number of client workstations (Bing, 2000).

A Mesh network makes use of mesh nodes. Mesh nodes connect with each other via the internet. Basically, a large number of devices of client workstations can be connected with each other via a large number of network access points. This is most useful in large scale network such as those in malls and city-wide network (Sourangsu & Chowdhury, 2013).

Client workstations connect to access points just like they do in an infrastructure network and form a mesh node. Each mesh node is connected using a routing protocol that transmit information among client workstations.

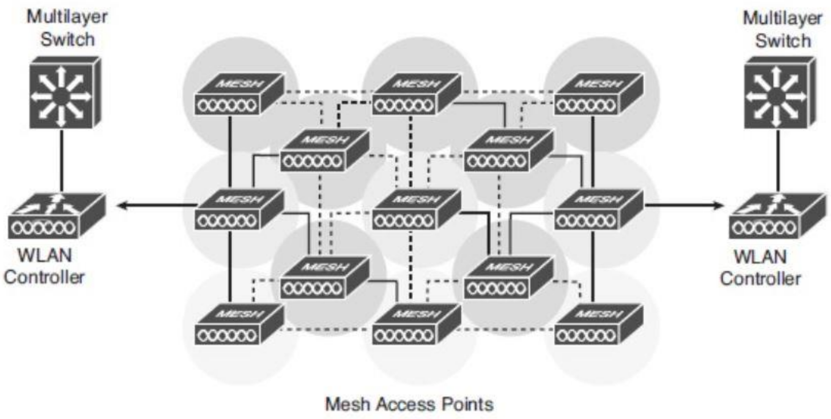


Image 6: An ESSs Extended Mesh Structure

3 WIRELESS NETWORK SECURITIES

3.1 Why do Wireless networks need protection?

For a LAN network to be functional, it has to be connected to a landline/cable line and then connected to a PC’s internet port which is not only costly but also unstable since the internet connection travelling through an internet cable is subjected to physical deterioration and damages. On the other hand, in a case of WLAN network, the only requirement is that the transmitter devices that broadcasting the wifi signal and the client device is inside the area covered by the WLAN signal. Controlling a LAN network is easy. The internet cable usually runs along buildings and it can be disabled by using a server management application (McQuerry, 2008).

There are, however, some risks associated with using WLANs. WLAN networks use and transmit wireless frequencies and go through physical obstacles such as concrete or brick walls. Therefore, their coverage is much wider than that of LAN networks, which are limited by cables and ports. A WLAN signal can therefore be found and accessed to even outside the buildings. That leaves opportunities for cybercriminal s to connect to and take control of an entire network from outside the building’s control centre. A practice called “WLAN eavesdropping" is the most obvious example of such risk (Ohrtman & Roeder, 2003).

In order to provide the most basic security measure for WLANs, two main components are needed:

Authentication: Decides who can use the network. Through user and control authentication, a network can identify and gives access to the person with the privilege (Ohrtman & Roeder, 2003).

Encryption: This method helps alter the information and data format that are broadcasted through the WLAN network and make it complicated for cybercriminals to understand and deduct any useful information from “eavesdropping" into the network (Ohrtman & Roeder, 2003).

3.2 WLAN Security

A WLAN generally has three main components: Wireless client, Access points and Access servers

- Wireless Client

In particular, a standard laptop or desktop computer with a NIC (Network Interface Card) installed can allow the wireless client itself to connect to the wireless network.

- Access Points (AP)

Provides wireless frequency signal in a certain area and connected to that WLAN.

- Access Server

Each access server acts like an EAS (Enterprise Access Server) that provides control and management methods for that WLAN. There are two structures in EAS: Gateway mode and Feedback mode.

Gateway mode: EAS is placed between AP and the rest of the enterprise network. An EAS controls all the bandwidth and data flow between LAN and WLAN and acts like a firewall.

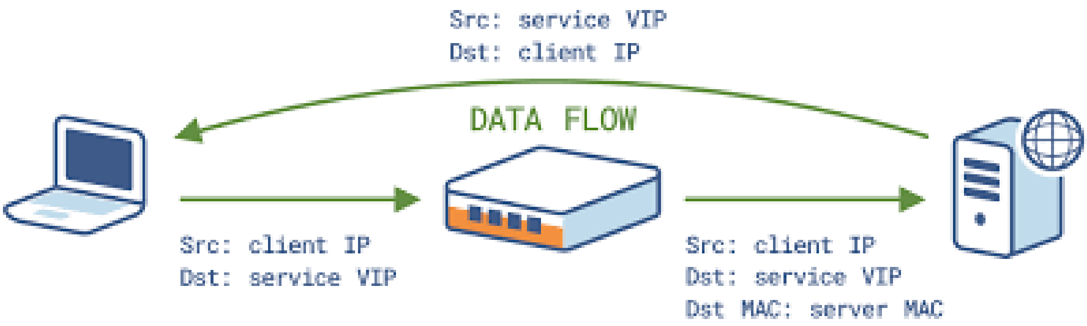
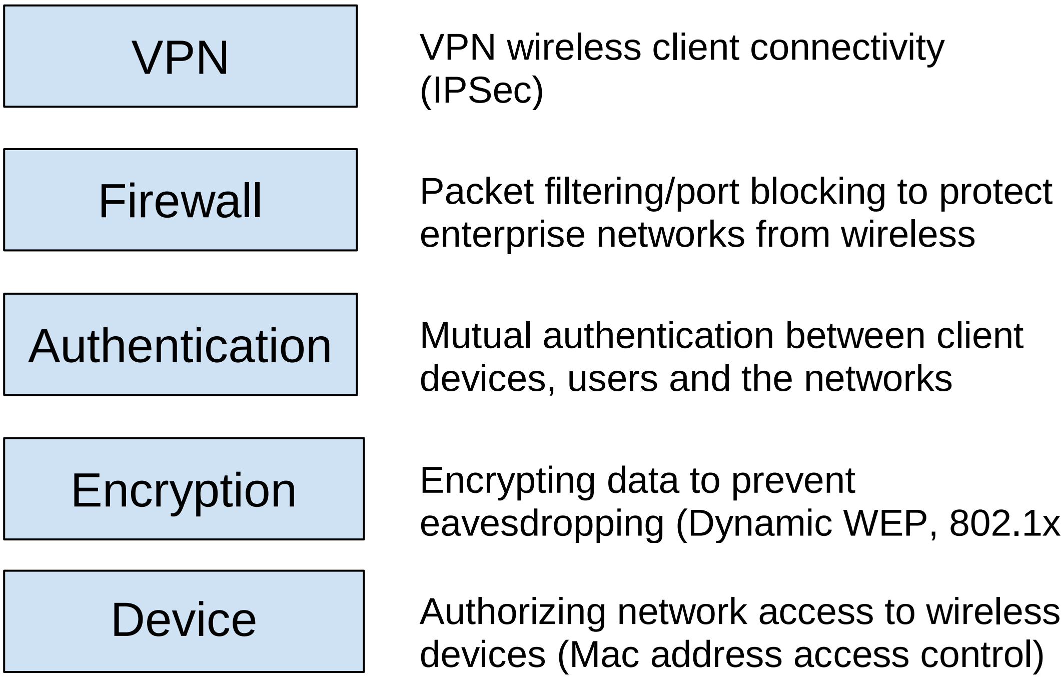


Image 7: EAS in Gateway mode

Control mode: Different than in Gateway mode, EAS controls APs and controls the wireless access but do not involve with user's data flow.

3.3 Security Structure

WLAN security structure supports an open-and-full-scale security model. There are five parts and each part can be configured by the administrator to meet the requirements and demands for each client.



VPN	VPN wireless client connectivity (IPSec)
Firewall	Packet filtering/port blocking to protect enterprise networks from wireless
Authentication	Mutual authentication between client devices, users and the networks
Encryption	Encrypting data to prevent eavesdropping (Dynamic WEP, 802.1x
Device	Authorizing network access to wireless devices (Mac address access control)

Image 8: A standard WLAN security structure

- Device Authorization

Wireless clients can be blocked via their hardware addresses (MAC address). EAS maintains a database of these wireless clients which are allowed to connect and their APs as well (Held, 2003).

- Encryption

WLAN also supports WEP (Wired Equivalent Privacy), 3DES (Triple Data Encryption Algorithm) and TLS (Transport Layer Security) standards. It is used to prevent unauthorized access. WEP locks can be created by per-user / per-session basic (Held, 2003).

- Authentication

WLANs use 802.1x EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) method in order to make sure only authenticated wireless clients are connected. EAS also uses a RADIUS (Remote Authentication Dial-in User Service) server which operated by digital certifications for increase maximum protection (Held, 2003).

- Firewall

EAS uses two firewall methods: Packet Filtering and Blocking based on IP address chains. From this configuration, a firewall can allow or block a wider range of data (Held, 2003).

- VPN

VPN stands for Virtual Private Network, using different protocols to secure and encrypt data such as:

  - IPsec (IP Security):

IPsec secures and protects network communication between hosts or operating systems (Gilbert, 2003).

  - SSL & TLS (Secure Socket Layer - Transport Layer Security):

The cause of SSL and TLS is to provide privacy and integrity of a connection. SSL is a certificate that ensure that the connection between hosts is encrypted. A SSL has two parts: a public key and a private key that are used to establish a secure connection. User information such as passwords, credit card number are encrypted when SSL is enabled (Held, 2003).

- PPTP (Point to Point Tunnelling Protocol):

PPTP allows users to extend its network by going through private connections known as “tunnels” over the public internet (Held, 2003).

4 ENCRYPTIONS

4.1 Definition

Encryption is a method that transforms and converts plaintext or any kind of data from readable into a ciphertext or an encoded version of that data. This is to make sure only the authorized sender and the designated receiver can read the data, to prevent eavesdroppers across the internet from getting sensitive information (Wilkins, 2011).

A common decryption method is the use of a key combined with the encrypted data to recover the original information, a method that has been used since the time of the Roman Empire but has now been more automatize and can process keys and cipher texts in a more rapid pace (Wilkins, 2011).

For example, “I am Bao” in encrypted text will look like:

eyJpdiI6Ik1NZEVjemU0QWtLOXlicWNRaXFhQ2c9PSIsInYiOjEsIml0ZXIi
OjEwMDAsImtzIjoxMjgsInRzIjo2NCwibW9kZSI6ImNjbSIsImFkYXRhIjoiIiwi
Y2lwaGVyIjoiYWVzIiwic2FsdCI6InVYa0o1U214ejJZPSIsImN0IjoiWU9jdEk
wV3VGNGVXbkhrK09TaXJSSjgwdnZQVkM4SUtMVkc0UHd1VGwzd1Nhc
HV0VGRkQ1lRVVN5VlFITEFocms4NHJVbzB2eTNLSUlnPT0ifQ==

Therefore, anyone eavesdropping cannot understand what the encrypted string means and sensitive information is well protected.

4.2 Classification

Encryption commonly has two distinguish cipher methods: Stream cipher and Block cipher.

4.2.1 Stream Cipher

Stream cipher is a method in which the cryptographic keys are applied by every bit / binary digit and one bit at a time. For example, a stream cipher can generate a 15-byte key to decrypt a frame and generate another 200-byte key to decrypt another frame (Wilkins, 2011.) Stream cipher is an efficient encryption method and it costs less computing resource. The image below describes stream cipher.

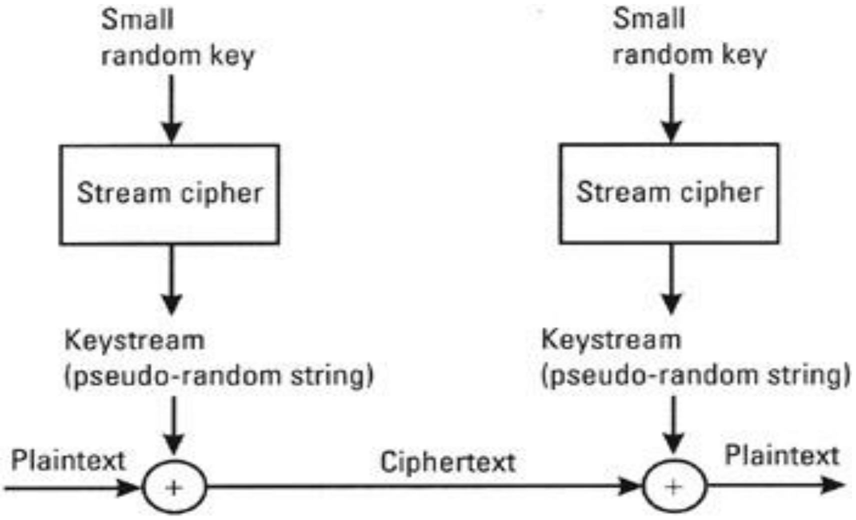


Image 9: A Stream Cipher Operation

4.2.2 Block Cipher

Block Cipher is different. A Block Cipher generates a single key with a predetermined length (64-bits, 128-bits, 192-bits, 256-bits).

Plaintexts that are unencrypted will be fragmented into “blocks” and those “blocks” will be independently mixed with the key. In the scenario that the plaintext block is not compatible with the key block, more random plaintexts will be added into the original plaintext block to achieve an encryption desirable size. Fragmentation and other procedures within this method will cost more computing resources (Gary, 2016).

This operation procedure is called ECB (Electronic Code Block). This operation possesses a vantage weakness that an input plaintext will always generate the same output cipher text. Attackers can take advantage of this to determine the plaintext from the ciphertext itself (Wilkins, 2011).

Below is how block cipher works:

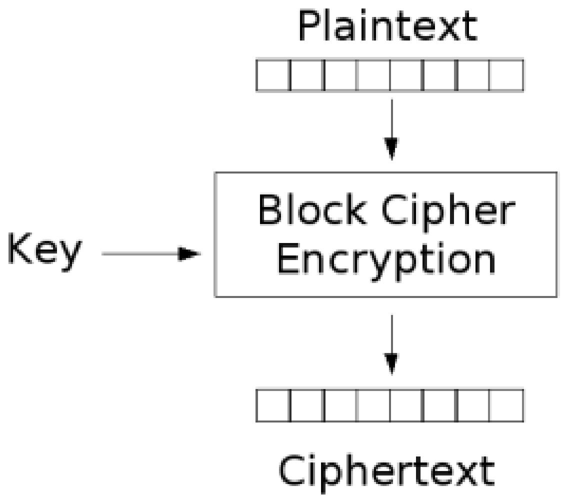


Image 10: A Block Cipher Operation

There are some encryption techniques that can overcome certain problems mentioned above:

- Using Initialization Vector (IV)

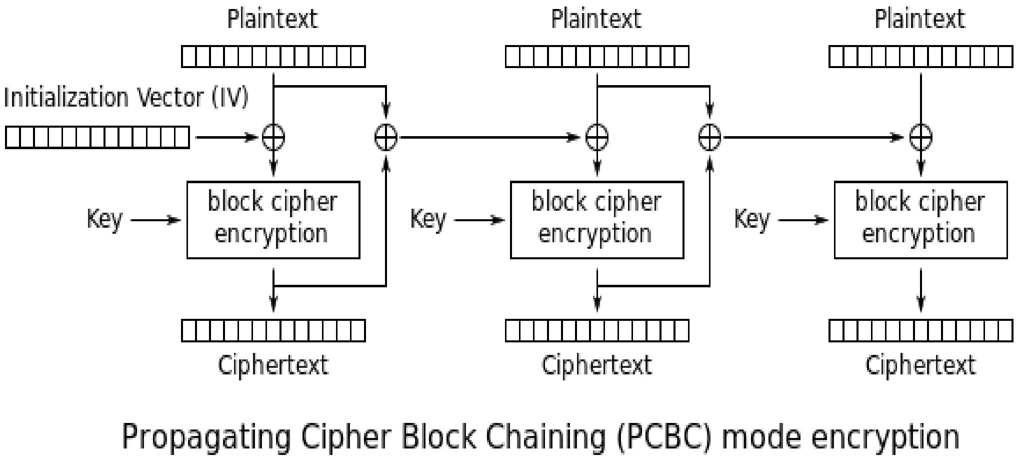


Image 11: The use of Initialization Vector

IV is added in order to change the cipher key. It is inserted right before the cipher key is generated. IV is random or pseudo random by requirement because random and pseudorandom is a critical and important condition to achieve security. When IV changes, the cipher key changes and the outcome is that there will be different ciphertext results.

- Feedback mode:

The Feedback mode improves the encryption procedure to prevent a plaintext generating the same ciphertext in a whole encryption operation. Feedback mode will make a block cipher into a self-synchronizing stream cipher (Held, 2003).

5 WEP AS A PROTECTION METHOD

5.1 WEP definition

WEP stands for Wired Equivalent Privacy, an algorithm created in order to protect information while it is in transfer. WEP prevents eavesdropping, unauthorized connection access and anti-jamming between transmissions.

WEP uses RC4 stream cipher along with a 40-bit code and a 24-bit Initialization Vector to encrypt information. Encrypted information is created using XOR Cipher Operation between keys and plaintext. Encrypted information and Initialization Vector will be sent to the designated receiver. The designated receiver then will decode the information base on IV and the WEP key already in possession (LANCOM, 2018).

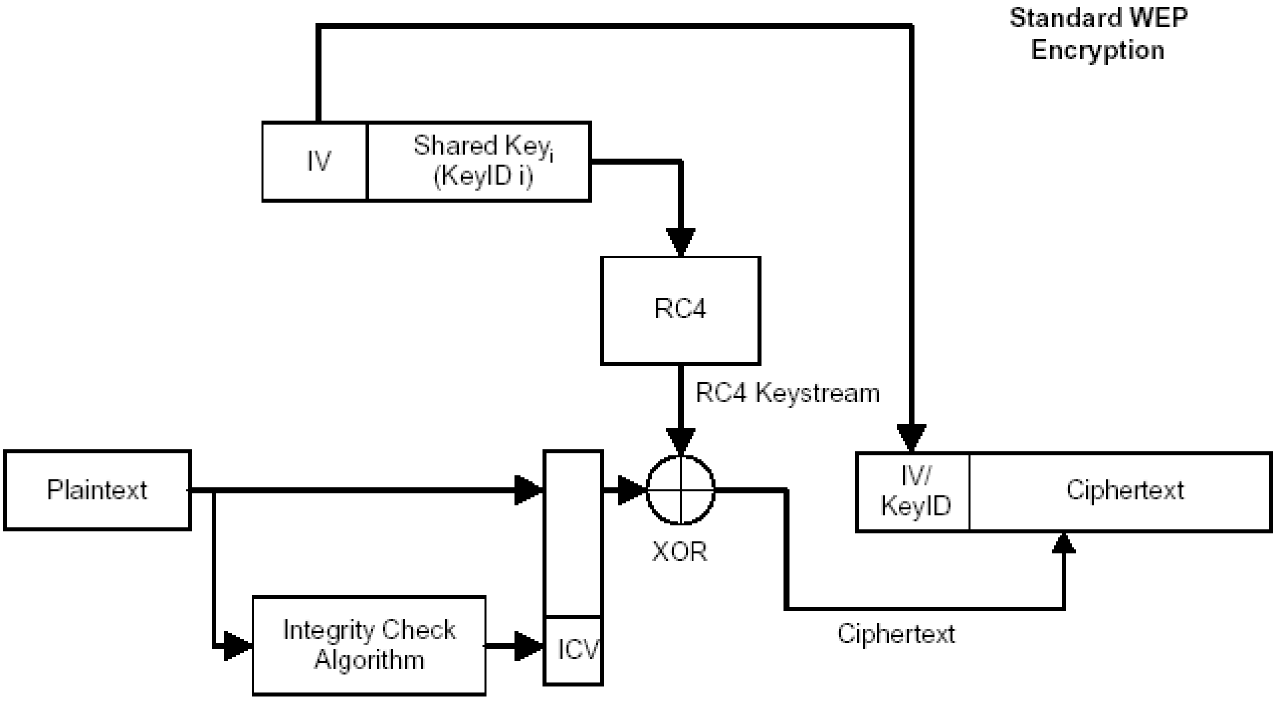


Image 12: Encryption using WEP

5.2 Frames that are encrypted by WEP

In order to skip ECB (Electronic Code Block) during encryption operation, WEP uses 24-bit IV. 24-bit IV is connected into WEP key before it is processed by RC4. The value of IV must be changed frame-by-frame so as to prevent conflicts. A conflict happens when there are the same IV and WEP key are being used, therefore only one key is used to encrypt the whole frame (NetSpot, 2018).

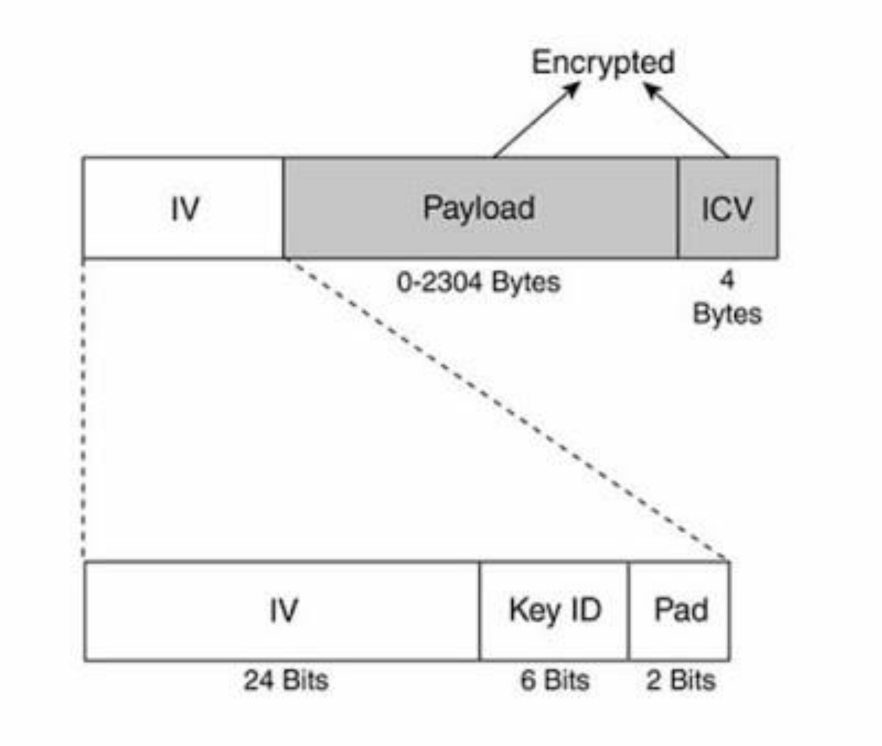


Image 13: Encrypted Payload and ICV

5.3 The procedure of encrypting and decrypting

The 802.11 standard requires WEP key to be configured on both client and Access Point. The WEP key in client must match the WEP key in AP so that the information can be transmitted. In a data frame, WEP encrypts:

- Payload: the transmit data itself
- ICV: Integrity Check Value

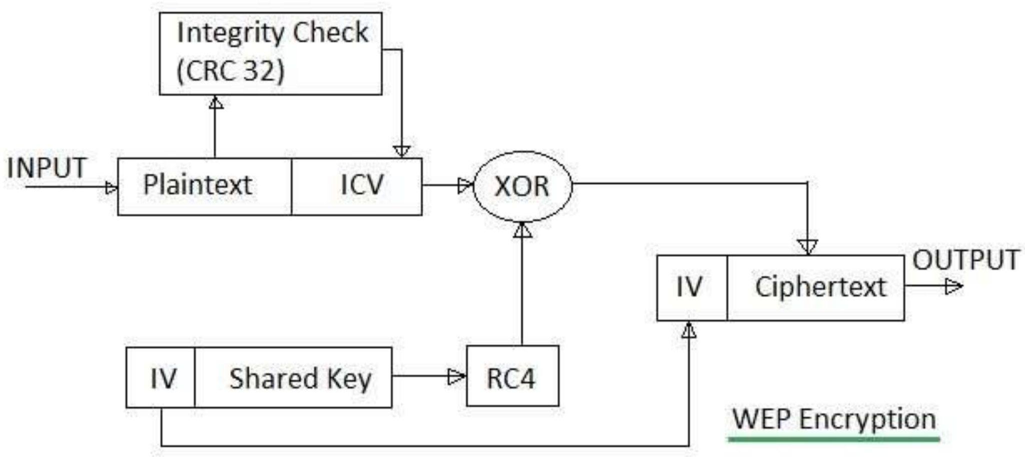


Image 14: The procedure of WEP encrypting and decrypting

A standard WEP Encryption method is shown above. The 802.11 standard provides a 32-bit ICV that has the ability to check the integrity of a data frame, this action is executed in order to make sure there is no error occurs during the whole transmitting process (NetSpot, 2018).

ICV is checked using the “bits error checking” CRC32 (Cyclic Redundancy Check 32). In the beginning, there will be a “broadcaster” that calculates a value and puts the result into ICV. Then ICV will be encrypted along with the data frame. After that the receiver receives the encrypted data frame and ICV, calculates the ICV value again and compares it with the original ICV value. If they match, that means the data frame was not changed or faked, if they do not match, that data frame will be deleted.

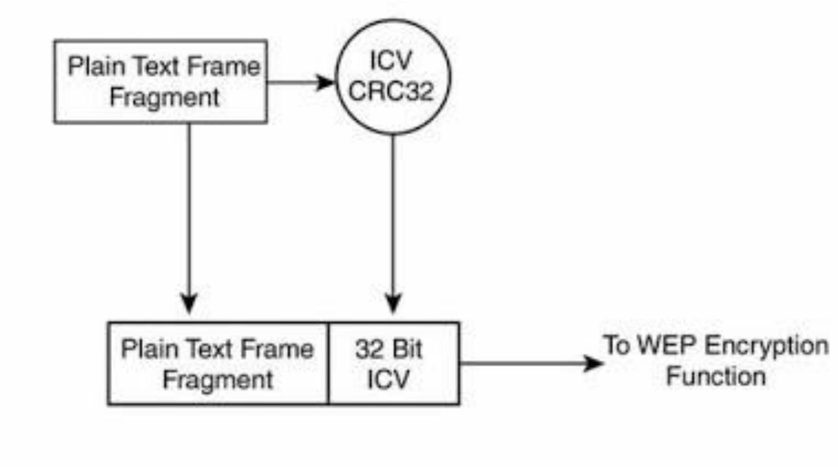

Plain Text Frame Fragment
ICV CRC32
Plain Text Frame Fragment
32 Bit ICV
To WEP Encryption Function

Image 15: ICV Cyclic Redundancy Check 32

5.4 Weaknesses of WEP

WEP uses a permanent key shared between an Access Point (AP) and Users with a random 24-bit Initialization Vector. Therefore, the same IV will be used many times and by collecting transmitted information, attackers will have enough information for cracking the WEP key that is in used (NetSpot, 2018).

When a WEP key is exposed, attackers can decrypt the transmitted information and can change the data inside the transmission as well. Using a permanent key between many users makes WEP an easy target for cyber-criminals. WEP also does not provide mutual authentication since WEP allows users to authenticate an AP but the AP cannot confirm the identity of users.

5.5 Solutions to maximize WEP

- Using a 128-bit WEP key:

Normally, WEP devices allow their keys to be configured at: 40-bit, 64-bit and 128-bit. Using a 128-bit key will increase the data package that cybercriminals need to collect for analyzing IV, 128-bit key will cause delays and prolong the time to crack the WEP key.

- Change WEP key regularly:

Changing the WEP key regularly to prevent the WEP key from being exposed while it is in use and make it harder for cybercriminals to focus on a single WEP key (Ilyas & Ahson, 2005).

- Using statistical data analysis tools:

Since WEP key cracking application needs to gather a large amount of data packages and cybercriminals may have to use a tool that boosts up the data package, there should be a booming in data package if someone tries to crack the WEP key. Using such statistical data analysis tool can help the server manager find out and apply counter-measures (Ilyas & Ahson, 2005).

6 COMMON WIRELESS ATTACK METHODS

6.1 Rogue Access Point

6.1.1 Definition

A Rogue Access Point is a wireless access point that is used/installed to cause confusion that affects the current WLAN. It is likely to be add by an employee or a cybercriminal (Ashley, 2016).

6.1.2 Classification

- Incomplete configured Access Point

An Access Point can become a fraud device during the configuring process. Changes inside the Service Set Identifier (SSID) of the WLAN itself will make the Access Point unable to authenticate connections that are unauthorized.

In a fabricated scenario, during OMA (Open Mode Authentication) process, wireless users are in "uncertified and unconnected" mode can send authentication requests to an Access Point and then if the Access Point certified that the users are legit, they will move to "certified and connected" mode. Rogue Access Point can cause confusion when certifying users' requests, making it delayed and vulnerable, cybercriminal s can send a large amount of "fake requests" that will overload the Access Point, make it denies every connection requests from all the users and disconnect users who are already connected (Zwicky et al, 2000).

- A fake AP from another nearby WLAN

Client's device using 802.11 standard will automatically pick the AP that has the most powerful signal. Therefore, certified users can connect to others nearby AP with the same clarification. Even though nearby AP does not attract nearby users’ connections but because of the automatic method of the 802.11 standard. These connections can make some sensitive information vulnerable (Ashley, 2016).

- A fake AP created by cyber-criminal

This is the classical “man in the middle” method, whereas the cybercriminal stands and steals data stream between two end points. This kind of attack is powerful since the cybercriminal can steals every data that are transmitted between the two end points.

It is very difficult to have a “man in the middle” attack in wired network because it is required to have an actual physical connection, but with WLAN, it is easier. The cybercriminal will create a fake AP point that is stronger than the real current AP (Ashley, 2016.) This AP fake can be created by copying every setting from the real AP’s configuration such as: SSID, MAC address…

The next step is to force users to connect to the fake AP. There are two common ways:

- Wait for the users to connect to the fake AP by themselves. This method will take more time and depends on the number of users (Ashley, 2016).
- Create a DDos (Denial of Service Attack) inside the real AP, then the real AP will overload and disabled. Therefore, all the connected users are disconnected from the real AP and with the 802.11 standard, their devices will choose the AP that has the stronger signal and that is the fake AP. This will ensure every user will connect to the fake AP (Ashley, 2016).

In order to make sure the second method will work; a hacker needs to ensure that the fake AP has the most powerful signal. Also, as stated before, the fake AP has all the features that the real AP has, so if a user connects to the fake AP, he/she is still accessible to the internet but the data transmitted from his/her device and the incoming information all have to go through the fake AP which is monitored and managed by the cybercriminal himself. Therefore, the hacker can get everything he wants through the fake AP (Miller, 2003).

- A fake AP created by an employee

Because of the convenience of the WLAN, some employees may configure themselves an AP and connect it into the company's wired network. By doing this, they just create a huge security breach in the network system since they do not have enough wireless security knowledge to create a powerful protection for their AP.

Hackers or strangers outside the company then can break the AP of the employee which is poorly secured, get a straight connection to the company's network and steal valuable and vulnerable information or use the company's network to attack another organization (Zwicky et al, 2000).

6.2 De-Authentication Flood Attack

The attacker determines that the targets are the wireless users and their own connections (the APs which they are connected to). A re-confirmation frame that request the AP to re-authenticate the connection is inserted by spoofing the front and the end MAC address point. Users while receiving the re-confirmation frame will think that comes from the original AP (Miller, 2003).

Evil Twin Access Point:

An Evil Twin AP is a counterfeit / forged AP that looks legitimate in the outside, but inside it is used as a tool for eavesdropping and phishing scams on WLANs. This method is used to steal passwords of naive and unsuspected users and use them for phishing / scamming purposes.

Fake Access Point

The attacker uses a tool that can send packages of beacon with a fraudulent MAC address and SSID to create many virtual Access Point. By doing this, it will mess up the user's wireless card since it does not know which Access Point is the legitimate one to connect to (Miller, 2003).

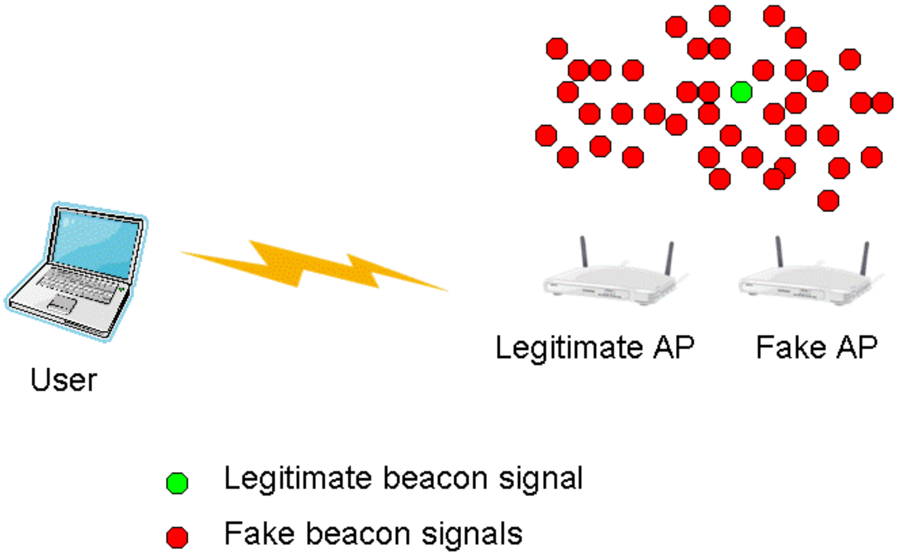


Image 16: Fraudulent APs and Legitimate AP

6.3 Disassociation Flood Attack

The attacker determines the targets are Wireless Clients because they are the bridge between the AP and users. Then the attacker sends out dissociation frame by faking the Source frame and Destination MAC address to the designated legitimate AP and its users.

Wireless Clients are also get this disassociation frame that forces the WLAN to shut down, the WLAN will think that this frame comes from the legitimate AP, it will automatically shut down and its users are blocked out also (Ashley, 2016).

Disassociation Flood Attack and De-Authentication Flood Attack

- Common:

Basically, they have the same attacking method, an arrow that fires two birds: AP and WLAN itself. More importantly, they keep attacking and attacking with fast pace like “flood”.

- Differences:

De-authentication: Force AP and Client to send the request frame => authentication failed.

Disassociation: Send Disassociation frame that make AP and Client believe that they have to shut down.

7 ANSWERING THE RESEARCH QUESTION

7.1 WLAN VPN

The VPN (Virtual Private Network) protects WLAN by creating a data blocking channel that blocks unauthorized accesses. VPN has a high reputation for its secrecy and protectivity.

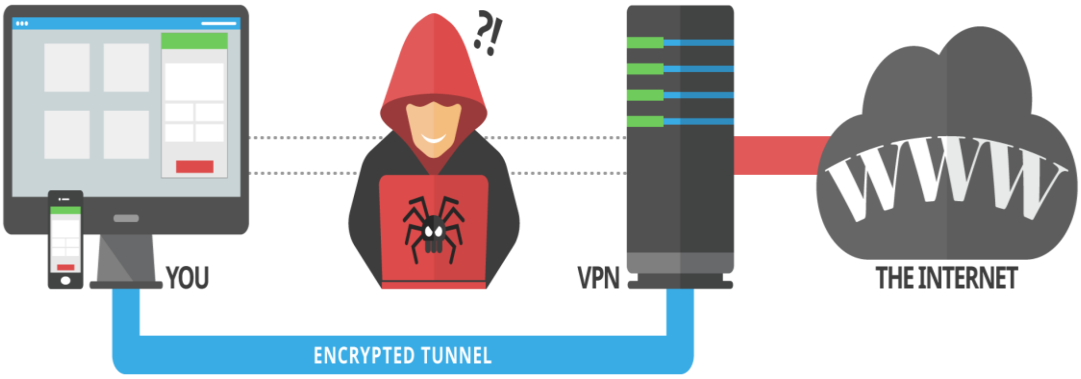


Image 17: VPN demonstration

VPN uses IPSec protection method. The IPSec uses strong algorithm such as Data Encryption Standard (DES), Triple DES (3DES) and Advanced Encryption Standard (AES) to encrypt data and uses other algorithm to certify data package. IPSec also uses digital key to authenticate public key (Gary, 2016).

A VPN basically protect every information that comes through its “tunnel”. In every security protocols, always come with encryption. Nowadays, most VPN services use AES method to encrypt data. There is AES 128-bit and AES 256-bit, the bit number stands for the key length and represents the possible number of combinations, it would take a few billion years for today’s fastest computer to crack an AES 128-bit key (Gary, 2016).

When a VPN is used, first the data go through the VPN server where everything cipher method happens and after that the VPN sends it to the designated server that the user wants to connect.

When user pings a server to a website, data are constantly sent back and forth over and over, but with a VPN in the middle, the user's request is the only thing goes through that website, the data move along the client and the VPN server, therefore the designated website/server does not hold anything sensitive of the user. VPN helps users "escape" out of cybercriminal s/ corporates / governments 's "eyes", secure the connection for users to browse the internet safely.

NO VPN
YOUR IP LOCATION
YOUR IP ADDRESS
YOUR EMAILS
WEBSITES BROWSED
EXPOSED!
WITH EXPRESSVPN
HIDE YOUR LOCATION
HIDE YOUR IP
ENCRYPT YOUR DATA
BROWSE ANONYMOUSLY

Image 18: VPN and without VPN comparison

7.2 TKIP and AES

- TKIP - Temporal Key Integrity Protocol

TKIP is a solution that was developed for IEEE standard, a WEP upgrades module so as to fix the internal security of the RC4 cipher. TKIP uses "hashing" IV against the counterfeiting data package, it also provides protocols to check the accuracy of each data package (Hucaby, 2005).

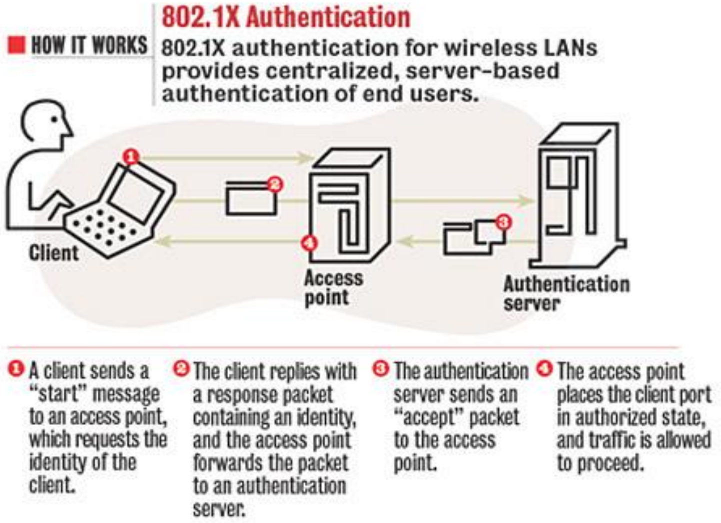
- AES - Advanced Encryption Standard

As mentioned above, AES was put into force by NIST (National Institute of Standards and Technology) - a non-regulatory of the United States Department of Commerce. AES uses CBT-CTR and CBC-MAC altogether and their combination is called AES-CCM. CCM is the combination of CBC-CTR encryption method and CBC-MAC integrity checking algorithm (Dubendorf, 2003).

7.3 802.1x and EAP

7.3.1 802.1x

802.1x is a special standard port-based Network Access Control (PNAC) connection which is designed by IEEE. 802.1x working environment is both wired and wireless, it provides a verification structure to the designated device. With IEEE 802.1x, when a user tries to log in into the server, that connection will be set in “blocked” status until the user’s authentication from the server is completed (Held, 2003).



■ HOW IT WORKS

802.1X Authentication

802.1X authentication for wireless LANs provides centralized, server-based authentication of end users.

1 A client sends a "start" message to an access point, which requests the identity of the client.

2 The client replies with a response packet containing an identity, and the access point forwards the packet to an authentication server.

3 The authentication server sends an "accept" packet to the access point.

4 The access point places the client port in authorized state, and traffic is allowed to proceed.

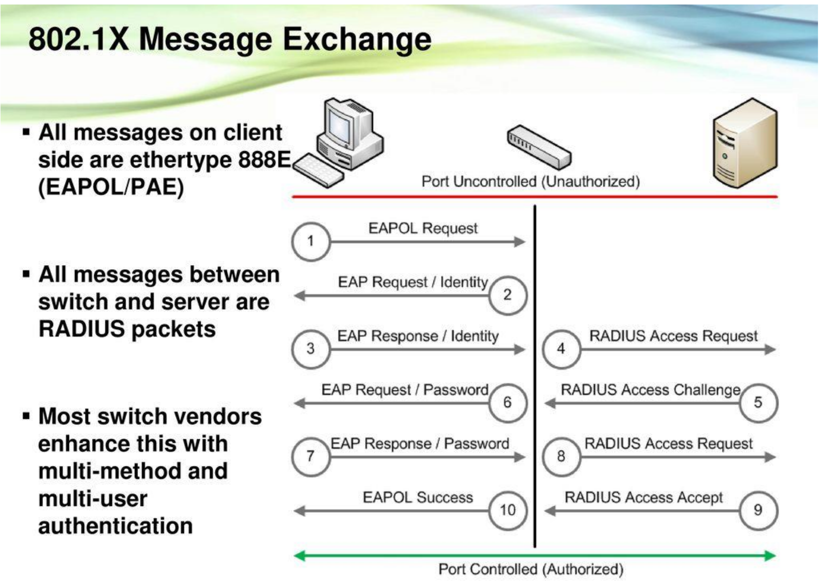
Image 19: 802.1x working procedures

7.3.2 EAP

Extensible Authentication Protocol is a authentication method which consists of:

User authentication: passwords, certificates

Handling protocol: MD5, TLS, OTP (One-time password)



802.1X Message Exchange

- All messages on client side are ethertype 888E (EAPOL/PAE)
- All messages between switch and server are RADIUS packets
- Most switch vendors enhance this with multi-method and multi-user authentication

Image 20: 802.1x-EAP working procedure

7.5 WPA (Wi-Fi Protected Access), WPA2 & WPA3

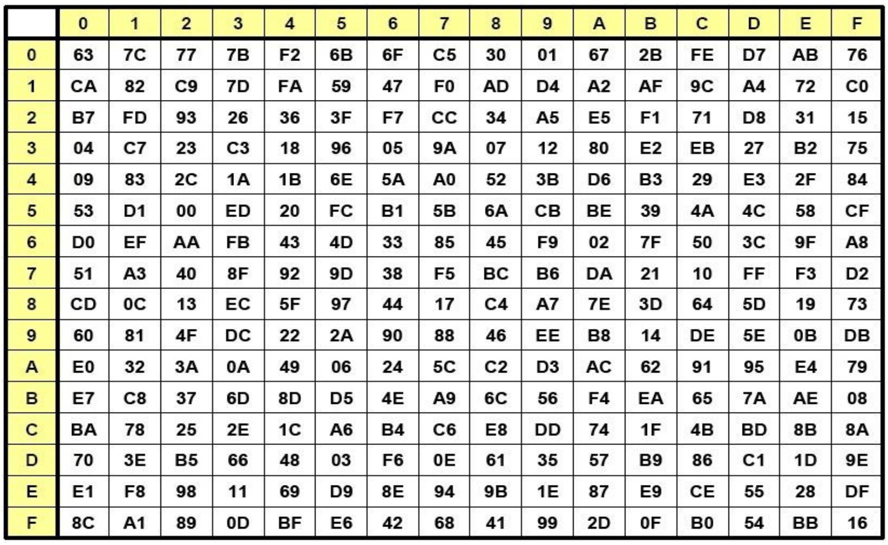
WEP is built to protect a wireless network from unauthorized access and eavesdropping. But not soon afterwards, errors and security breaches have been discovered. Therefore, WPA is built, develop and upgrade WEP's weaknesses

- WPA disadvantage

The most identical weakness of WPA is that it cannot handle Denial-of-Service or DoS attack. A hacker can disrupt the WPA Wi-Fi by sending at least two data packages with a wrong encryption key every second. Also, problems occur when there are too many passwords and shared contents between many users and vulnerable to password cracking attacks (NetSpot, 2018).

- WPA2 (Wi-Fi Protected Access 2)

On the long run, Wi-Fi Alliance has approved the IEEE 802.11i Enhanced Security or known as WPA2. This standard uses AES technology, this AES takes the cryptographic algorithm symmetry based on Rijndael S box: 128-bit, 192-bit and 256-bit key, providing extra protection and secrecy (NetSpot, 2018).



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Image 21: A Rijndael S box

- WPA3 (Wi-Fi Protected Access 3)

In January 2018, the Wi-Fi Alliance announced that WPA3, a new replacement for the old WPA2, has been developed. WPA3 will have a standard 192-bit security suite along with the CNSA (Commercial National Security Algorithm) which is intended for industrial, military and government applications (Wi-Fi Alliance, 2018).

WPA3 for the home and offices applications will increase privacy on public premises Wi-Fi networks and provide more protection layers to prevent cyber-attacks. Also, WPA3 supports easier authentication method and connection for devices without a screen for example Amazon Echo, Google Home or Xiaomi Home (Wi-Fi Alliance, 2018).

7.7 Filtering

Filtering is a basic security protocol that can be used along with WEP. Filtering works like an Access list on the router. It blocks the unwanted contents and allows the desired contents to pass through. There are two basic filtering methods in WLAN:

- SSID filter
- MAC address filter

7.7.1 SSID filter

SSID filtering is a basic filtering method and it can only be used in basic connections. SSID of the client must match with the AP SSID in order to authenticate and connect. Since it is the most basic filtering method, it is also the most vulnerable, easy to get hacked. There are some mistakes that WLAN users tend to have when managing SSID:

- Using the default SSID value, this create opportunities for hacked can trace the MAC address of the original AP
- Using SSID that related to a company sensitive information
- Using SSID as a protection method for a company / organization

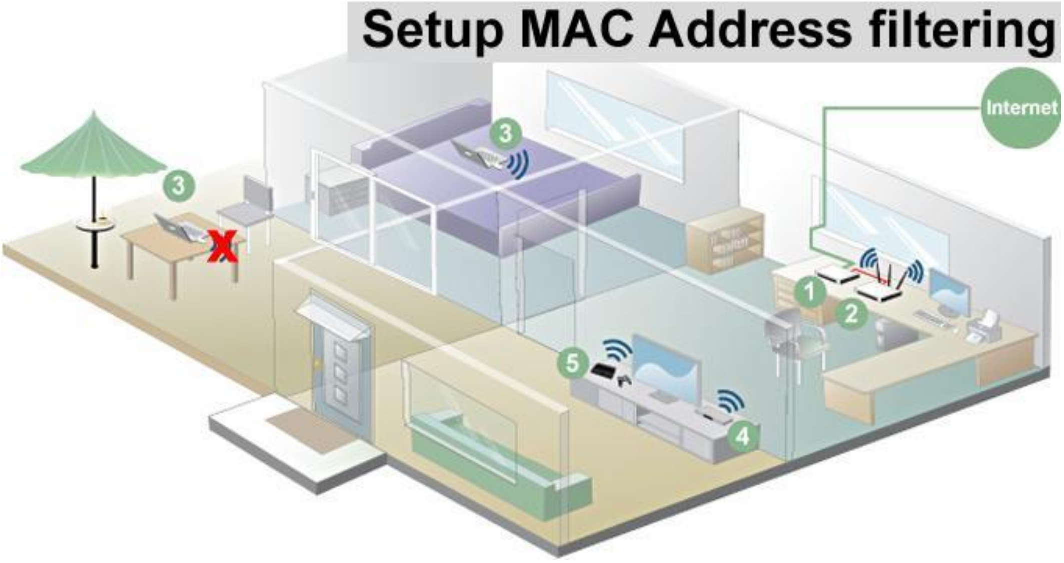


Image 22: MAC Address filtering demonstration

7.7.2 MAC Address filter

Almost every AP has the ability to filtering MAC address. The server manager can build up a list of allowed MAC addresses, it will improve the WLAN security by limiting the MAC addresses that can participate into the network.

Any devices with a right certification (SSID) can authenticate with the WLAN router and participate into the network. MAC address filtering method adds one more protection layer to this. Before allowing the device to connect to the network, the router will check the device's MAC address first and see if the device has a MAC address that does not appear on the

MAC address filtering list of the AP, AP will not grant permission for that device to connect to the server (Miller, 2003).

8 DISCUSSION AND CONCLUSION

8.1 Limitations

The information provided in this thesis focuses mostly on WLAN security theories and approaches that are customized to match the needs of medium-sized public premises and businesses. The methods mentioned in the thesis may be applicable for private residential WLAN units due to their relatively comparable sizes and simplicity of installation and use. In addition, the same category of cybercriminal that may try to attack the medium public premises and businesses that are data phishing and petty financial crime types may also try to target small household units for the same purposes. However, the level of technical complexity in this thesis may not be suitable for non-technical readers who may not have enough knowledge in the field.

The research papers do not anyhow intend to provide any in depth or guidance for large scale industrial setting since the level of advancement at such installations are beyond the scale of the included content in this paper. In addition, cybercriminals that may try to attack such large installations are usually corporate thieves or spies. They have different purposes and methods as well as the level of backups in terms of technology and legal aid as well as access to confidential data. In short, they are beyond the level of comprehension of this thesis.

8.2 Reliability and Validity

This thesis uses information and references from published articles, printed books and other sources of information. It is also collated against comparable works in the same field and the same subject. Therefore, it is safe to assume that the research paper provides an accurate piece of work in term of information validity. This thesis uses standard English and technical terminology to ensure that anyone with technical training can understand it with ease. Moreover, even novices in the field can benefit from the content.

8.3 Suggestions for further research

The author does not wish to provide a work that is too highly academic. Therefore, this thesis is useful for small-sized companies. A future study could be made to benefit other types of companies.

8.4 Conclusion

WLAN technology has been developing rapidly, with more and more characteristics and configurations to support bigger bandwidths, easier in installation and meet technological and economic demands. In addition, wi-fi now also helps users to gain access from almost every public premise such as travel stations, parks, airports…

Regarding WLAN, it is important to focus on WLAN security because WLAN can be an easy target for hackers/cybercriminals to steal valuable information. Therefore, along with the rapid development of WLAN's functionalities, protecting WLAN from dangerous threats is also important. This improves work productivity and creates trust in users.

Building a network with a perfect security solution is very difficult. Based on the actual size of the network, as well as the level of security required, comes with various security set up methods and security mechanisms. Depending on the home network, school, public access point or corporate environment, there are different security measures to fit with each suitable scenario.

REFERENCES

Printed sources:

Bing B. 2000. High - Speed Wireless ATM and LANs. London, the United Kingdom: Artech House Publishing.

Bing B. 2001. Wireless LANs and Home Networks: Connecting Offices and Homes. The United Kingdom: World Scientific Publishing Co Pte Ltd.

Dubendorf V. A. 2003. Wireless Data Technology. USA: John Wiley & Son Publishing.

Harte L. 2004. Introduction to 802.11 Wireless LAN (WLAN). USA: Althos Publishing.

Held G. 2003. Securing Wireless Lans. USA: Wiley Publishing.

Hucaby D. 2005. Cisco ASA and PIX Firewall Handbook. USA: Cisco Press.

Ilyas M. & Ahson S. 2005. Handbook of Wireless Local Area Networks - Applications, Technology, Security and Standards. USA: CRC Press.

Miller S. 2003. Wi-Fi Security. USA: McGraw-Hill Education.

Ohrtman F. & Roeder K. 2003. Wi-Fi Handbook Building 802.11b Wireless Networks - Wi-Fi Security. USA: McGraw-Hill Education.

Zwicky E D., Cooper S. & Chapman B. 2000. Building Internet Firewall. USA: O’Reilly.

Digital sources:

Ashley. C. 2016. Types of Wireless Network Attacks. Phoenixts [accessed 17 April 2018]. Available at: https://phoenixts.com/blog/types-of-wireless-network-attacks/.

Gary S. 2016. WLAN Security: Best Practices for Business Wireless Network Security. Built-in Chicago [accessed 13 April 2018]. Available at: https://www.builtinchicago.org/blog/wlan-security-best-practices-business-wireless-network-security.

LANCOM System GmbH. 2018. WPA and private WEP settings. Lancom systems [accessed 15 April 2018]. Available at: https://www.lancom-systems.com/docs/LCOS-Refmanual/10.00-Rel/EN/Referenzhandbuch_7.60_EN/WLAN/aa1615892.html.

McQuerry S. 2008. Wireless LANs: Extending the Reach of a LAN. Cisco Press [accessed 05 April 2018]. Available at: http://www.ciscopress.com/articles/article.asp?p=1156068&seqNum=3

Nayak K J. & Singh P. 2015. Fundamentals of Research Methodology. Research Gate [accessed 18 April 2018]. Available at: https://www.researchgate.net/profile/Jayanta_Nayak2/publication/309732183_Fundamentals_of_Research_Methodology_Problems_and_Prospects/links/582056a208aeccc08af641dc/Fundamentals-of-Research-Methodology-Problems-and-Prospects.pdf.

NetSpot. 2018. Wireless Security Protocols: WEP, WPA, and WPA2. Net Spot [accessed 16 April 2018]. Available at: https://www.netspotapp.com/wifi-encryption-and-security.html.

Sourangsu B. & Chowdhury R. 2013. On IEEE 802.11: Wireless LAN Technology. Arxiv [accessed 20 April 2018]. Available at: https://arxiv.org/pdf/1307.2661.pdf.

Walliman N. 2011. Research Methods The Basics. Edisciplinas [accessed 17 April 2018]. Available at: https://edisciplinas.usp.br/pluginfile.php/2317618/mod_resource/content/1/BLOCO%202_Research%20Methods%20The%20Basics.pdf.

Wi-Fi Alliance. 2018. Wi-Fi Alliance introduces security enhancements. Wi-Fi Alliance [accessed 04 May 2018]. Available at: https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements.

Wilkins S. 2011. WLAN Authentication and Encryption. Plural Sight [accessed 07 April 2018]. Available at: https://www.pluralsight.com/blog/it-ops/wireless-encryption-authentication.

Image sources:

Image 1: https://www.pinterest.co.uk/pin/468937379933205100

Image 2: http://www.conceptdraw.com/solution-park/computer-and-networks

Image 3: https://www.indiamart.com/proddetail/long-distance-outdoor-wireless-network-installations-7685877848.html

Image 4: https://www.howtogeek.com/141257/htg-explains-how-does-bittorrent-work/

Image 5: https://damayanthiherath.wordpress.com/a-survey-on-ieee-802-11-wireless-lan-standards-and-physical-layer-issues/

Image 6: https://www.networkcomputing.com/wireless-infrastructure/wireless-lan-models/1308618959

Image 7: https://www.haproxy.com/support/technical-notes/an-0053-en-server-configuration-with-an-aloha-in-direct-server-return-mode-dsr/

Image 9: https://www.globalspec.com/reference/81191/203279/2-6-stream-ciphers

Image 10: https://courses.cs.ut.ee/2016/infsec/fall/Main/DataEncryption

Image 11: https://crypto.stackexchange.com/questions/29134/precisely-how-does-cbc-mode-use-the-initialization-vector

Image 12: https://nullsec.us/wep-overview/

Image 13: http://wirelesslansite.blogspot.fi/2009/12/encryption-in-80211-standard.html

Image 14: http://www.rfwireless-world.com/Terminology/WEP-vs-WPA-vs-WPA2.html

Image 15: http://wirelesslansite.blogspot.fi/2009/12/encryption-in-80211-standard.html

Image 16: https://www.cse.wustl.edu/~jain/cse57107/ftp/wireless_hacking/index.html

Image 17: https://buffered.com/faq/what-is-vpn/

Image 18: https://www.expressvpn.com/what-is-vpn

Image 19: https://www.networkworld.com/article/2285891/security/8-no-cost-low-cost-tools-for-deploying-802-1x-security.html

Image 20: http://slideplayer.com/11865358/66/images/8/802.1X+Message+Exchange+All+messages+on+client+side+are+ethertype+888E+%28EAPOL%2FPAE%29+All+messages+between+switch+and+server+are+RADIUS+packets..jpg

Image 21: https://captanu.wordpress.com/tag/decryption/

Image 22: http://geekntech.com/howto/tplink-mac-address-filtering/