# Wireless networking and malicious association computer science

Wireless security is to prevent unauthorized user to access the wireless network or damage the computer by using wireless network. When the wireless technology has been first introduced to the world, it already has few danger methods that will harm the user’s desktop or laptop, but that time cracker and hacker don’t have any resources to crack or hack a network by using wireless technology. At that time, the wireless network only use by the big company. But now day, wireless network is very common, every corner of the world like cafA©, shopping mall, school, or college that has provide wireless access for the people to access it. Not only cafA© and college using wireless network, at other country it use wireless technology to connect whole city’s network.

With this technology, people that around the wireless router can easily to access the wireless network to do the search of the information, check mail or play online game. Because of the wireless technology, now day, every laptop has wireless adapter card pre-install inside and make the laptop more portable and let them can connect to internet easily. Not only for laptop, wireless technology also make benefit for the desktop. Desktop can connect to network by installing a wireless adapter card or plug in an USB wireless adapter then desktop can connect to a network and without cable messy around the floor. In this case, wireless technology has become widely use and because of this reason, the risk of using wireless technology has increase and let many hacker found the way to hack the wireless network. All of security risk is related to the current wireless protocol and encryption method.

Most of the wireless networks use IEEE 802. 11b for standard communication and IEEE 802. 11b have already became standard wireless networking technology among the small business user and home user. The IEEE 802. 11b can support the indoor distance from several meter to several hundred meters, and can support the outdoor from several kilometer to several ten of kilometers by using unlicensed wireless band. Now day, the wireless network devices normally are equipped with Wired Equivalent Privacy (WEP) data encryption. WEP data encryption was based on 64-bit RC4 encryption algorithm. Other that 64-bit RC4 encryption algorithm, 128-bit encryption algorithm is another data encryption on the WEP data encryption. But this kind of device is more expensive compare with 64-bit RC4 encryption and beside that, all the nodes must use the same encryption level.

1. 2 Aim of Research

Aim of the research is to implement the wireless security into the CSC System to prevent unauthorized user to access the wireless network.

To increase the security level of the wireless network.

To avoid the data or information inside the server or computer been hacked by unauthorized user.

To increase the safety of the data transfer between server and computer.

To add extra encryption method to encrypt the packet need to be transfer.

To prevent unauthorized user to shut down whole system though the wireless access point.

Chapter 2: Main Body2. 1 Wireless Security Concept

A research has been carried out about the concept of the Wireless Security and how to enhance the wireless security. Wireless Security is to prevent an unauthorized user to invade the server database and bring harm to entire network. Below are the results of the research.

2. 1. 1 Unauthorized Access

According to the research, have a lot of way to break into the wireless access point without an authorization. The unauthorized access will cause company’s daily operation failure and lose profit. Below are the some of the examples unauthorized accesses.

2. 1. 1. 1 MAC Spoofing

MAC spoofing is a technique to change an assigned MAC (Media Access Control) address to another different MAC address. When a person using this technique, he/she has his/her reason to changes a network device’s MAC address, whether is legitimate or illegitimate. Changes a network device’s assigned MAC address allows bypass the access control list on the server or router, either hiding a computer on a network or attacking a network by simulate another network device.

MAC spoofing occurs when a cracker or hacker has the ability to listen the network traffic that passed by and through it; the cracker or hacker can identify the MAC address of the computer with network privileges. Most of the wireless system allows MAC filtering to only allow authorized computer that with specific MAC address to access the network. The computer that

don’t has specific MAC address can’t access the network, so the cracker or hacker use a program which has network “ sniffing” capability and combine with other software or program to pretend the computer has any MAC address that the cracker desires. (Wikipedia, 2010)

2. 1. 1. 2 Malicious Association

The Malicious Association is hacker that can connect to company network by using their cracked laptop. This type of laptop is known as “ soft AP (Access Point)” and this type of laptop is created by using some software that makes the hacker laptop’s wireless adapter card look like a legitimate access point. After the hacker has already gained the access to the company network, the hacker can steal the password or plant the computer virus into the network. (Wikipedia, 2010)

2. 1. 1. 3 Ad-hoc Network

Ad-hoc network, also known as peer-to-peer network built up between two or more wireless computers and these wireless computers don’t have access point in between them. Ad-hoc network usually provide little protection, encryption method to the network. When a company or person using Ad-hoc network and wired infrastructure network together at the same time, and will link up a secured network to an unsecured network.

Connect two different network topology need to have a bridge between them. Bridging is in two forms. User can connect the network topology y a direct bridge and indirect bridge. Direct bridge need to configure by the user and indirect bridge is user share resource on the user computer. The indirect

bridge is provides two security problems. The first problem is the data can be obtained through the secured network on the user computer and this data exposed to other user discovery via the Ad-hoc network bypassing the user secured network. The second problem is a Trojan, computer virus or worm can be placed on the user computer through the Ad-hoc network. The unauthorized user no needs to crack the password of the network and can place the computer virus through the Ad-hoc network. (Wikipedia, 2010)

2. 1. 1. 4 Denial of Service

C: UsersZoukyDesktop424px-Stachledraht_DDos_Attack. jpg

DoS (Denial of Service) or DDoS (Distributed Denial of Service) will occurs is when an attacker continues non-stop bombards an attacker targeted access point with bogus request, failure messages, or other commands. Denial of service will cause other users can’t get into the network and also will cause a network crash. The DoS attack will expose a little bit of the data to the attacker, when the DoS attack happen, the interrupted network will prevents the data flow and also indirectly prevent the data from being transmitted. After the DoS attack has been performed, the attacker will start to observe recovery of the wireless network. During the initial handshake code is start to re-transmitted to the wireless network, the attacker continue what he remain. The attacker will record down the initial handshake code and use cracking tools to analyze the security weakness and exploit this code to get an unauthorized access to the system. (Wikipedia, 2010)

2. 1. 1. 5 Man-in-the-middle Attack

Man-in-the-middle attacker using a computer to sets up a soft AP (Access Point) and enticing other computers to log into the computer that already been sets up to soft AP. After this all are done, the attacker connects to a real access point by using other wireless card and the attacker will offers a steady flow of the network traffic through the done hacking computer to real network. Man-in-the-middle attack forces other computers' AP drop the connection to real network and reconnect to attacker's soft AP. This allows hacker to receive what other computers want data need to send out to real network. (Wikipedia, 2010)

2. 2 Basic Security for Wireless

Wireless network exist in this world already has a decade, at that time the security for the wireless network still not strong enough to prevent infiltrate by hacker or cracker. But at that time the hacker doesn't familiar on technology or technique to hack the wireless network. One of the reasons is the hacking device to hack the wireless network still hard to achieve on that time market. After a decade, the technology and technique to hack a wireless network and the step to build up the hacking device can found on internet. So now day the wireless network users need to have a strong and better wireless security to secure the wireless network. Below are the basic securities for wireless network for the first wireless network has been introduced.

2. 2. 1 Service Set Identifier

SSID (Service Set Identifier) is a common network name for a device in a wireless LAN and some of the wireless device has its own default SSID. The

default SSID can be replaced by other string and normally this string is generated randomly. SSID is to identify a name for particular wireless access point. All wireless network need to have SSID within the wireless access point just can communicate each other. The client doesn't know the SSID of the access point, then that client can't simply access the network; this is to prevent hacker to invade network by access through access point. The hacker need to know the SSID of a network just can complete the 802. 11b protocol to access the network. The access point will broadcasts the SSID by the beacon inside the wireless device. However, even the broadcasting of the access point is turn off, the SSID still can detected by hacker with undetected monitoring of particular network or " sniffing". So, all the clients need to know the SSID of the access point before can make connection to the wireless device.

(Bhagyavati, Wayne C. Summers and Anthony DeJoie, 2004), (Prasad, 2007)

2. 2. 2 Medium Access Control Address Filter

Each wireless access point can be configured only accept the client's MAC address that already registered inside the wireless access point. With this function, the network administrators can limit the access of the client into wireless network by register the client's MAC address into the wireless access point. Most of wireless device's MAC address is unique and MAC address filter only allow the client's MAC address already registered in the wireless access point to access the network. The entire client's MAC address will store into MAC address ACL (Access Control List) and wireless access

point will denied other wireless device if the wireless device’s MAC address is not register inside wireless access point’s MAC address ACL.

(Bhagyavati, Wayne C. Summers and Anthony DeJoie, 2004), (Prasad, 2007)

2. 2. 3 Wired Equivalent Privacy

WEP (Wired Equivalent Privacy) is intend to give wireless users have a security scheme is equivalent to the wired network security. WEP doesn’t provide any superior level or higher than that level of security, although WEP doesn’t has superior level of security but it security level is equivalent with wired network. In the practice, the result show that the security level of WEP need to equivalent to wired network security is hardly to achieve. The use of WEP is to prevent the wireless client from sending and receiving data from the wireless access point, the wireless clients need to have the correct WEP key just can connect to the wireless access point. Now mostly of the network devices is equipped with the WEP data encryption and the encryption algorithm for the WEP is 64-bit RC4. Some of the network device capable to uses 128-bit encryption algorithm. After WEP is active, each 802. 11 packet will encrypted by 64-bit RC4 key with RC4 cipher stream. This key is composed of 24-bit IV (Initialization Vector) and other 40-bit is WEP key. IV is chosen by the sender and the IV can be change, this make every packet won’t encrypt with the same key. Another additional 4-byte is for ICV (Integrity Check Value); ICV is computed and appended on the original packet. RC4 cipher stream is generated by 64-bit RC4 encryption algorithm. The WEP encryption algorithms work on a key that share between wireless device and wireless access point. The packet is encrypted by using the key

before packet is send out and all packets won’t have same cipher stream. The packet receiver use integrity check to ensure that the packet is not modified during the transmission. Most of the systems are share a single key among all the wireless device and wireless access point. The Integrity Check Field is to ensure the packets are not been modified during the transmission and Integrity Check Field also encrypted with the RC4 cipher stream. WEP is using CRC-32 (Cyclic Redundancy Code – 32) mechanism for integrity check. CRC is defined as a class of “ checksum” to prevent overflow by dividing the message into binary.

(Bhagyavati, Wayne C. Summers and Anthony DeJoie, 2004), (Halil Ibrahim BulBul, Ihsan Batmaz and Mesut Ozel, 2005), (Prasad, 2007)

2. 3 Comparison between SSID, MAC Address Control Filter and WEP

From the research, SSID (Service Set Identifier), MAC (Medium Access Control) address control filter and WEP (Wired Equivalent Privacy) are the basic security for the wireless network. This three security methods can implement together in one network. Because these are basic security for wireless network, so the security methods are easy to break by unauthorized user. If not implement other security methods and only just implement SSID, MAC address control Filter and WEP into wireless network, that wireless network will not secure under protection of these three security methods.

The wireless access point will broadcast the SSID to the wireless client and wireless client just can access to the access point. When the access point broadcast its own SSID, the entire nearby wireless client will know the SSID of that network or access point, even the unauthorized users also will know

the SSID of the network. The unauthorized users will attempt to access the wireless access point. And the wireless access point can close the SSID broadcast function; mean that the SSID is hidden. But when the authorized user requires connecting to the access point, the authorized user will broadcast the SSID to the wireless access point, if the SSID broadcast by the authorized user is match with the SSID of the access point. The authorized user just can make connect to the access point. This make hacker a chance to hack the access point because when authorized user is broadcasts the SSID to the access point, hacker can capture the packet that broadcast by the authorized user and make connection to the wireless access point.

The wireless device’s MAC address will store inside the wireless access point ACL (Access Control List), the wireless device’s MAC address need to be match with MAC address inside the wireless access point ACL just can connect with wireless network. If that wireless network has more than 20 computers need to connect to the wireless network, then the network administrator need to enter all the computers MAC address into the wireless access point ACL. This will make the network administrator very troublesome enter the MAC address one by one and MAC address can be forged.

WEP has been considered as a failure in wireless security, at the end it still accepted by the IEEE because WEP wasn’t aim for provides fully security for wireless. WEP encryption is very easy to crack by the unauthorized user. WEP only authenticates the wireless client. This allows an unauthorized user to capture the packet send by the wireless client. WEP key is easily lost or stolen by unauthorized user and if the stolen WEP key hasn’t been report to the network administrator, the network administrator won’t able to detect

the unauthorized user has already infiltrated the wireless network. If the stolen WEP key has been reported, network administrator require to change the entire devices that have use the same WEP key with stolen device’s WEP key. If the company or enterprise has more than thousands of wireless user using that wireless network, this can be a very difficult task for the network administrator to change the entire WEP key for each wireless users.

Like just mentioned, the WEP authentication message is easy to forging by the unauthorized user. Unauthorized user can capture the authentication message that send by the wireless client and forge a new authentication message; unauthorized user can use this forged message to associate with wireless access point. The management for WEP key in not specific in WEP standard. Since don’t have management for WEP key, then WEP key will be use for a long term and lack of quality. Most of the wireless network uses one WEP key and share between the entire network and the entire wireless client’s access point need to program with same WEP key. Because of this reason, network administrators rarely change the WEP key.

SSID, MAC address control filter and WEP is basic security for wireless network; these methods still can’t apply in wireless network. Just using SSID, MAC address control filter and WEP are not enough to prevent the security break. These methods require associate with other security methods to enhance the wireless security to prevent security break.

2. 4 Advanced Security for Wireless

From the research that carried out, advanced wireless securities are to replace the basic wireless security and improve what basic wireless security vulnerability.

2. 4. 1 Wi-Fi Protected Access

WPA (Wi-Fi Protected Access) is a certification program that created by Wi-Fi (Wireless Fidelity) Alliance; WPA is a subset of the IEEE 802. 11i. This technology is designed to response to the weaknesses that found in WEP. WPA will generate the key based on the master key and the master key never use by WPA. To encrypt the data, WPA is much more secure than WEP.

Key management and updating in WEP is poorly provided, the secure key management is a built-in function in WPA. Mean that WPA can update and manage the key easily, not like WEP. If WEP need to manage or update the key, the network administrator needs to change entire wireless client key that has connection with the wireless network. WPA got one key only and that is master key like just mentioned, network administrator only require to change that master key then WPA will generate the key based on the master key. Generated key is hierarchy of the master key. So this make the management and updating become much easier.

The IV (Initialization Vector) values can be reuse and the length of the IV is become longer, from 24-bit increase to 48-bit. Another additional part, the IVs are the sequence counters for the TSC (TKIP Sequence Counter), to protect the loop of the data. The WEP message integrity protocol CRC-32 has been proved ineffective. Because of this reason, WPA uses a MIC (Message Integrity Check) mechanism to replace the WEP message integrity protocol.

The correct MIC is very difficult to guess. (Halil Ibrahim BulBul, Ihsan Batmaz and Mesut Ozel, 2005), (Bhagyavati, Wayne C. Summers and Anthony DeJoie, 2004), (DifferenceBetween, 2010)

WPA has 3 improvements over WEP:

Improved Data Encryption

WPA improves the data encryption through the TKIP (Temporal Key Integrity Protocol). TKIP generates the key by using hashing algorithm and adding the integrity checking feature, this will ensure the key haven’t been edited by other person. TKIP is a Temporal Key hash Function and it is another option to WEP to fix all security problems that WEP has and it doesn’t require installing other new hardware. TKIP same like WEP, use RC4 stream cipher to encrypt and decrypt data and all involved clients require share the same key. This key must be 128-bit and it calls Temporal Key (TK). The Initialization Vector also include in TKIP. Even if the TK is shared among all the wireless clients, all wireless clients generate different RC4 key stream. Since the communication participants perform a 2-phase generation of a unique Per-Packet Key (PPK), which is used as the key for the RC4 key stream. (Halil Ibrahim BulBul, Ihsan Batmaz and Mesut Ozel, 2005)

User Authentication

User authentication in WPA is through the EAP (Extensible Authentication Protocol). This function is missing in WEP and WEP access to the wireless network is based on computers network card’s MAC address and MAC address is very simple to be stolen. The purpose of EAP is to create a more

secure public-key encryption system to ensure that only authorized user can access the wireless network. (Halil Ibrahim BulBul, Ihsan Batmaz and Mesut Ozel, 2005)

Integrity

WPA has a new mechanism call (MIC) Message Integrity Code for TKIP is computed by a new algorithm, name “ Michael”. MIC is computed to detect errors in the data contents, either is transfer errors or purposely change the data content. The “ Michael” is a 64-bit MIC and need to add to the data and ICV (Integrity Check Value). (Halil Ibrahim BulBul, Ihsan Batmaz and Mesut Ozel, 2005)

2. 4. 2 Robust Security Network

RSN (Robust Security Network), also call as WPA (Wi-Fi Protected Access) 2. At year 2004, concept of RSN has been released, where the wireless devices need to support by additional capabilities. RSN is fully tested by Wi-Fi Alliances. RSN has a whole new standard and architecture to utilize the IEEE 802. 1X standard for AES (Advanced Encryption Standard) and access control. RSN is using a pair-wise key exchange (Four Way Handshake) protocol, RSN also utilizing with 802. 1X for key management process and mutual authentication. Now, 802. 11i allows for the network implementation and also can use TKIP (Temporal Key Integrity Protocol). By default RSN uses CCMP (Counter Mode MAC Protocol) and AES (Advanced Encryption Standard) to provide for a scalable and stronger solution. AES is a replacement for RC4.

Data transmission between the wireless access point and wireless device, RSN uses encryption algorithms and dynamic negotiation of authentication on the data transmission. The authentication of RSN is based on 802. 1X and EAP (Extensible Authentication Protocol). Encryption algorithms and dynamic negotiation of authentication make RSN's security more secure and save. RSN is stronger and better than WEP and WPA because RSN is using dynamic negotiation, 802. 1X, EAP and AES. Unfortunately only the latest devices have the capability let RSN to accelerate the speed of algorithm's calculation in wireless client and wireless access point; now day of wireless product can't fully provide the performance of RSN.

(Halil Ibrahim BulBul, Ihsan Batmaz and Mesut Ozel, 2005), (Bhagyavati, Wayne C. Summers and Anthony DeJoie, 2004), (DifferenceBetween, 2010)

2. 5 Comparison between WPA and WEP

WPA (Wi-Fi Protected Access) is the solution for the WEP vulnerability, has some critics done for the WEP, the WPA has numerous enhancements over WEP. WPA's TKIP encryption algorithm has fully enhances the WEP's RC4 encryption algorithm. TKIP make the data encryption more efficient and replace the RC4 vulnerability. WPA has made the key management became much more easier compare with WEP, because the WEP's key require enter one by one to the wireless client, if the company has more than thousands users then the network administrator need to enter more than thousands keys into the users' computer. If the key is hacked by unauthorized user, then network administrator need to change key for entire company's computers. On the other hand, WPA no needs so troublesome, WPA only

needs to enter one master key, and then WPA will generate key according with the hierarchy of master key, after that WPA will assign the key to the clients and the key is generated in 48-bit of IV size. Even the company got more ten thousands users also no need to trouble the network administrator. If one of the key has been hacked by unauthorized user, TKIP just need to generate a new key then network administrator can info the wireless client to change the key.

WPA has EAP to authenticate the wireless user. WEP is using MAC address to authenticate the wireless user and some of the wireless device’s MAC address can be forged. If the wireless device’s MAC address has been forged by unauthorized user then the unauthorized user can easier to connect the wireless network without known by the network administrator. Network administrator also won’t notify the wireless network is infiltrated by the unauthorized user until the wireless user report there is a missing MAC address. WPA is using EAP to authenticate the wireless user and the EAP for each wireless client is hard to forge by unauthorized user. If the EAP of the client is forging, but the unauthorized user still need wireless clients private key just can access the wireless network.

WEP don’t have error checking for the data content, and this will cause the looping of the data. If can’t prevent replay attacks and will cause the wireless network crash. WPA has inserted the MIC into TKIP and IV sequence mechanism; this is to prevent replay attacks in the wireless network. MIC and IV sequence mechanism support for the existing wireless infrastructures not require installing new wireless device. Adding MIC and IV sequence mechanism without install new wireless device, adding these two methods

can increase the wireless security and also without increase the installation cost of wireless device.

Compare WPA with the WEP, WPA has solved a lot of WEP vulnerabilities. This make WPA is more secure compare with WEP because WEP only is basic security for the wireless network; it doesn’t provide any protection for the wireless network. WEP’s security methods can let a small enterprise to setup a small wireless network. For the big company, WEP’s security methods are hard preventing the unauthorized access from outsider.

2. 6 Comparison between WPA and RSN

For now, never the less, RSN (Robust Security Network) is the strongest wireless security protocol for the wireless network. RSN provide stronger data encryption algorithm and all advantages of WPA. The RSN data encryption algorithm method is using AES (Advanced Encryption Standard) to encrypt the data. What advantages WPA have all included in RSN, expect the RSN data encryption algorithm is more advance.

For WPA require upgrade for the software and firmware of the wireless device for the existing wireless network infrastructure, but the RSN doesn’t support existing wireless network infrastructure, require upgrading the wireless device in order to implement AES. Implement RSN into the existing wireless network infrastructure require extra cost for just upgrade the hardware.

RSN need large amount of processing resources in order to protect the wireless network. Mean that implement RSN will reduce the wireless network performance by processing the data transfer or verify the wireless client.

2. 7 Table of Comparison between WEP, WPA and RSN

Below is summary of the comparison between WEP, WPA and RSN:

Features of MechanismWEPWPARSNEncryption Cipher Mechanism

RC4

RC4 / TKIP

AES / CCMP

CCMP / TKIP

Encryption Key Size

40 bits

128 bits

128 bits

Encryption Key Management

None

802. 1x

802. 1x

Encryption Key Per Packet

Concatenated

Mixed

No need

Encryption Key Change

None

For Each Packet

No need

IV Size

24 bits

48 bits

48 bits

Authentication

Weak

802. 1x – EAP

802. 1x – EAP

Data Integrity

CRC 32 – ICV

MIC (Michael)

CCM

Header Integrity

None

MIC (Michael)

CCM

Replay Attack Prevention

None

IV Sequence

IV Sequence

(Halil Ibrahim BulBul, Ihsan Batmaz and Mesut Ozel, 2005)

Chapter 3: Conclusion3. 1 Achievement of Objectives3. 1. 1 To increase the security level of the wireless network.

In chapter 2. 2 until 2. 4, the different wireless securities provide different service.

3. 1. 2 To avoid the data or information inside the server or computer been hacked by unauthorized user.

In chapter 2. 1, the type of the unauthorized user that can infiltrates the wireless network and chapter 2. 2 and 2. 4 the methods to prevent hacking.

3. 1. 3 To increase the safety of the data transfer between server and computer.

In chapter 2. 2 until 2. 4, increase the safety of the wireless access point of wireless network.

3. 1. 4 To add extra encryption method to encrypt the packet need to be transfer.

From chapter 2. 2 until 2. 4, the extra encryption methods that can hide the data detail.

3. 1. 5 To prevent unauthorized user to shut down whole system though the wireless access point.

In chapter 2. 2 until 2. 4, the methods to prevent the unauthorized user to connect with wireless access point.

3. 2 Research Conclusion

A research has been carried out to finish this seminar report by studying the type of the unauthorized access, concept of the wireless security and how efficiency is the wireless network security by determine the wireless security method. Now wireless has already became widely use by company or enterprise, even at home also can using wireless to connect to internet for home purpose like surfing the internet. The reason why so many people like

to use wireless network compare with wired network, is because the structure of wireless network is more neat and easy to manage.

At the time wireless just came out to the market, the security for the wireless still breakable by hacker or cracker but need a lot of resources to break the security of wireless network. Because last time, wireless network just introduced, the hacker or cracker lack of technology and technique to break the wireless network. Still after few years, the technology and technique to break the wireless security can found in internet. At that time the wireless network has sound the alert and organizations are finding the solution for solve the wireless security problem. But now, the new technology of wireless security has out to market and the security methods are easy to install. So, now wireless security is not a problem.

In the report got mentioned is RSN can be the most dependable wireless security for the wireless network. But it still has certain problem like higher cost. Installation for the RSN needs to change whole wireless network infrastructure. WPA got a lot of security methods that can’t compare with RSN but WPA still dependable just like RSN. Doesn’t mean the expensive item is the good item. As long as the item is reliable then that item is a good item.