Man-in-the-middle Attacks Detection Scheme on Smartphone using 3G network

Jaemin Lee
School of Electronic Engineering
Soongsil University
Seoul, Korea
dlwoas@ssu.ac.kr

Chaungoc Tu
School of Electronic Engineering
Soongsil University
Seoul, Korea
chaungoctu@ssu.ac.kr

Souhwan Jung
School of Electronic Engineering
Soongsil University
Seoul, Korea
souhwanj@ssu.ac.kr

Abstract— **In this paper, we propose a scheme to detect the man-in-the-middle attacks occurring when user accesses to the Web server with SSL using smart-phones. Normally, server verification process under smart-phone environment does not properly work in computer environment. Because Mobile Web Server usually uses server-side certificate, and smart-phone cannot correctly validate server certificate, this could cause the risk of man-in-the-middle attack. This vulnerability allows a rouge AP to carry out a man-in-the-middle attack easily every time user connect to the secure website using his smart-phone via WLAN. To solve the problem in an effective way, we first make use of the dual interfaces network (3G and WiFi) in smart-phone to communicate with server in order to get certificates from both interfaces. The certificates are then compared to determine whether there is a man-in-the-middle attack or not. Our scheme not only offers a realistic countermeasure to prevent man-in-the-middle attack but also does not require a complex procedure or changes in HTTPs protocol.**

Keywords -- MITM; Rogue AP; Smart Phone.

I. INTRODUCTION

Nowadays, the developing of WiFi service has brought the increasing of smart-phone users who get benefit from its features. However, WiFi users still suffer from the risk of man-in-the-middle (MITM) attack. Based on users' habit of familiar SSIDs connect to an AP, a rouge AP can trick user to connect to its network by creating a WLAN with the same SSID with legitimate AP. By successfully luring users into its network, rouge AP can sniff and steal user packets through various types of attacks and modify those packets into various forms. One of the typical examples for those attacks is SSL interception. SSL interception can be implemented when user request to access secure Web server (which use the HTTPs protocol). By capturing and replacing the certificate with its own, a rouge AP can provide user with a fake certificate, thus can create shared session keys with user and server. With those session keys, a rouge AP can easily catch all the packets that contains personal information like user ID and password. This type of attack can be more easily applied to the mobile web environment where certificate verification process is not properly executed. To solve this problem, the proposed scheme takes advantage of the 3G network combining with existing WiFi network in user's smart-phone to provide a proper authentication method. To immediately detect the sign of MITM attack under secure connection, our scheme provides a method to verify the server's certificate in user terminal.

This paper is organized as follows. In Section II, we present various types of MITM attacks and current solutions for preventing the attacks. Section III describes the procedure and features of proposed scheme. The implementation of proposed scheme will be presented in Section IV. The experiments and results as well as comparison with other schemes are presented in Section V. Finally, Section VI provides concluding remarks.

II. RELATED RESEARCH

The phrase "man-in-the-middle" is used to describe the attack which occurs during communication between a consumer and a legitimate organization. The most dangerous part of man-in-the-middle attack is the ability to perform packet sniffing through encrypted communications between two sides [1] [2] [3] [4]. Recently, with the grown of smart-phone users, the risks for them to become victim of MITM attack have also become an issue in online communities.

In this section, we present different approaches of MITM attacks which are usually carried out by attacker before implementing SSL interception procedure and the solutions for defending against those attacks.

A. MITM attack types

1) MITM attack through the rogue AP

This is a kind of MITM attack which known as "session hijacking attacks" [5] [6] [7]. In this attack, the intruder aims to tamper the legitimate user's session by gaining access to it. The attacker usually start an attack by sniffing and eavesdropping techniques on a network stream, and ends with altering, forging or rerouting the intercepted data. This MITM attack is usually chosen by attacker to attack against public-key cryptosystems by substituting the intercepted public key with their forged public keys. In this case, the victim parties are made to believe that they are still under safe communication with each other. In common

MITM attack scenario, attacker often insinuates into the communication between a client and a server and transmits deceitful messages between them to make them feel safe in communicating with each other. Technically, attacker usually uses a program which appears like a server to the client or vice versa. Figure 1 illustrates that client/server scenario:

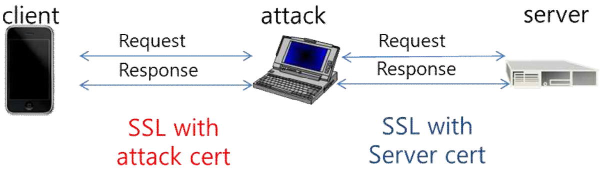


Figure 1 Client/server scenario

In MITM attacks, the attacker first aims to interfere the two sides of communications, and captures all communication between them. After successfully implementing the first step, attacker can launch other attacks like sniffing the packet, hijacking authenticated sessions, injecting packets or commands to the server, and sending the forged to the victim client. Main target of MITM attack is to get sensitive and valuable information, so MITM attacker frequently choose to intercept both HTTP and HTTPs communication. A MITM attack which can deceitfully direct the target endpoint (like the victim) to the attacker's proxy server instead of the real server can be considered as a successful attack. Objectives for MITM attacks include gaining access to the client's message and modifying it before forwarding to the server. The consequences for a successful MITM attack are misleading the communication, or getting confidential information like identity, address, password for malicious purposes.

With those potential threats, MITM attacks is a common risk to web-based financial transaction system. For example: e-business websites, payment gateways, and online banking, insurance and credit card servicing platforms. MITM attacks may lead to identity thefts and financial frauds.

2) *MITM attack through the Evil Twin*

This MITM attack is mainly based on the use of scanning and interfering methods [8]. By detecting the user connection with legitimate AP, the attacker can determine and create an AP with the same MAC address as legitimate AP. The attacker then tries to interfere with the connection between user and his current AP by sending the Disassociation frame. Using stronger of signal, the fake AP can successfully attract user to connect to it. The MITM attack is successful after user connects to the fake AP.

3) *MITM through the ARP Spoofing*

An attacker repeatedly send ARP reply messages to both sides of communication (user side and the legitimate AP side) attempt to associate his MAC address with the IP address of a target host, so that any traffic meant for the target host is redirected to the attacker's MAC instead [9].

4) *DNS spoofing*

In this attack, the ID of any DNS request is sniffed and target request is replied by attacker with the incorrect ID before the real DNS server. There are many existing tools for implementing this kind of attack. For example: "ADM DNS spoofing tools" which can spoof DNS packet actively and passively. Others knowable tools are "ettercap","Dsniff", DNS local spoofing, DNS jizz spoofing and DNS ID Spoofing also can be used for DNS spoofing.

5) *IP address spoofing*

In order to conceal the identity of the packet sender or to impersonate another computer system, the attacker creates IP packets with a forged source IP address. Although using this method on remote system can be very difficult because it requires the modification of thousands of packets at a time, it is still effective where trust relationships exist between endpoints. A typical tool for spoofing IP datagrams is "Hping" which only with one-line of command, this tool can send spoofed datagram to almost any target victim.

In such scenarios, a MITM attacker usually intercepts the communication to get exchanged public keys between client and server, so that he can modify those keys. The attacker also intercepts the relevant encrypted messages and responses, then uses the correct public keys to decrypt and re-encrypt them for all communication segments in every moment to successfully avoid any suspicion from either relevant party. Although such attacking seem too tough to accomplish, it can pose a real risk to insecure networks (e.g., the Internet, and wireless networks)

B. *MITM defense techniques*

1) *Detecting Rogue AP using Client-side bottleneck bandwidth analysis*

This method determines whether the network packets of an IP address are routed from APs, according to client-side bottleneck bandwidth [10]. The inter-arrival of Packet is derived from bandwidth. This value can be used to detect the difference between wired and wireless bandwidths. However, as this method has large window size problem and bandwidth measurement technique, it is not easy to be used in real environment.

2) *A Passive Approach to Rogue AP detection*

The main idea of this approach is based on the use of RTT to detect rouge AP and legitimate AP [11]. The characteristics of lower capacity and the higher variability between wired and wireless networks can be used for distinguishing between those networks. However, in different conditions, normal user can be accidently classified into an attacker.

Copyright (c) IARIA, 2012. ISBN: 978-1-61208-204-2

3) Using radius authentication server for prevent Rogue AP

This method uses the radius authentication server which is made from 4 parts: Wireless security management interface, database, radius authentication server, and rogue AP detection module [12]. Radius authentication server is used for device authentication. The problem of this method is the need for ISP (Internet Service Provider) to install the Radius authentication server, which causes inconvenience. This method cannot detect the rouge AP coming from an ISP which does not install the Radius authentication server.

III. DETECTION SCHEME

With the information provided in section II, we can easily see that user's privacy is still at risk even if they access through a secure service like SSL-based HTTPS secure connection service [5][6][7].

To solve this problem, many techniques have been proposed, however because of the cost, space limitations, facilities and feasibility, we cannot provide safe services to users [10][11][12]. The proposed technique provides a simple, user-side verification without significant cost increase for detecting the man-in-the-middle attack based on SSL interception. In order to find the attacker, we also do not need to install additional equipment and modify the existing protocol. This method is also likely to detect the attacker with no space limitations, which means we can detect the rouge AP anywhere.

In the proposed scheme, user terminal (like smart-phone...) requests the server certificate via 3G and WiFi networks simultaneously. Smartphones usually have 3G interface and 3G network is more security than WiFI [13]. After receiving the certificates, the user terminal verifies whether they are the same. If an attacker modified their server certificate through WiFi that will be detected in user terminal. This procedure is illustrated in Figure 2 below:

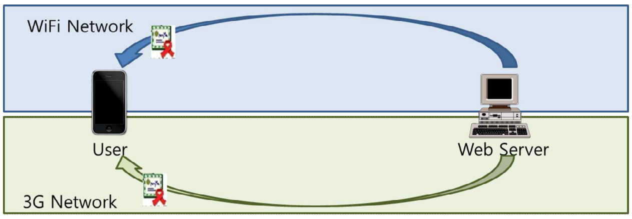


Figure 2 certificate transport using 3G network and WiFi network

The certificate of the web server where user frequently connects can be downloaded in advance via 3G networks and stored in user terminal.

Table 1 describes the structure for storing certificate value

TABLE I. TABLE FOR STORED CERTIFICATE VALUE

Web Site name	Certificate value	Save Date
paypal	b01aefc4c…..	2011.10.5
google	a330f91a1s…..	2011.6.20

Certificate values can be stored in PEM format or DER format. With PEM format, certificate values are stored in the form of base-64 encoding (base64 encoding) like numbers, letters and symbols etc …. With DER format, certificate values are stored in binary value form.

Figure 3 illustrates the comparison between certificate values in PEM format

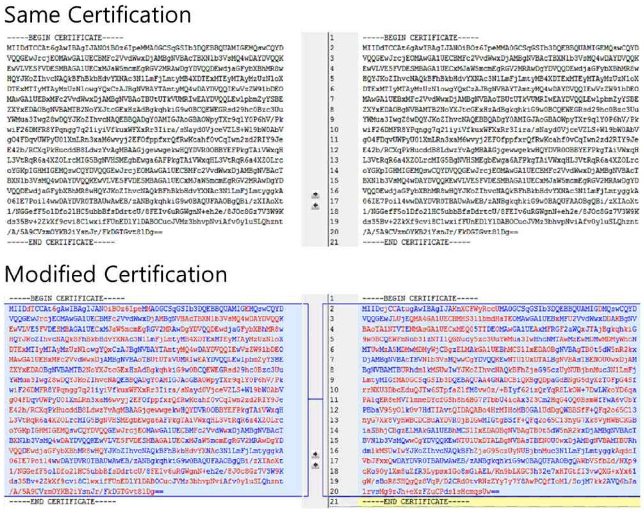

Same Certification
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
Modified Certification
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----

Figure 3 Certificate value verify in PEM format

In case two values are different, current AP will be considered as rouge AP and will be disconnected. The application will try to connect to other AP and restart the verification procedure. If there is no safe AP around, only the 3G network is used.

Figure 4 illustrates the verification procedure of our scheme.

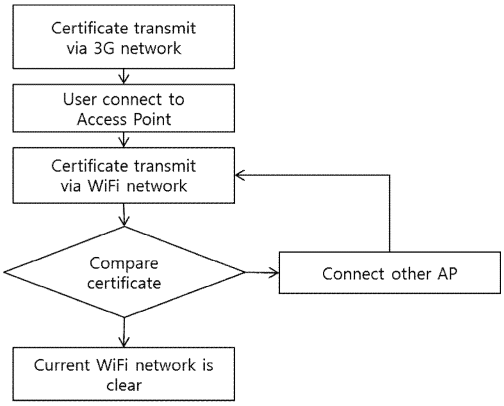

Certificate transmit via 3G network
User connect to Access Point
Certificate transmit via WiFi network
Compare certificate
Connect other AP
Current WiFi network is clear

Figure 4. Compare certificates received by 3G and WiFi

The verification procedure only runs at the first time when user connects to an AP. After the first verification to determine whether the AP is a safe one to use or not, if the AP is safe, all checked AP in the future don't have to repeat this procedure. Even connection another Web server service. This purpose is detect MITM AP.

IV. Implementation

In this paper, we implement the actual experiment for the proposed design techniques to defend against man-in-the-middle attacks to analyze the effective of our scheme. The architecture of our implement is illustrated by Figure 5 as follow

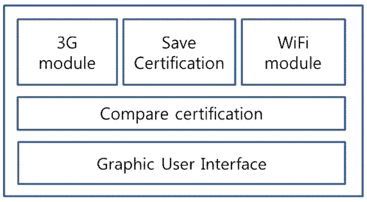


Figure 5 Application architecture of detect MITM attack

The implementation of our propose techniques is based on Android-based smart phones. An application is installed in Android phone to test the detection applications. The smart-phone device uses API 10 version 2.3.7, below are details of our experiment device:

- OS：Android 2.3.7 API 10
- Phone name: HTC Desire
- CPU: Qualcomm Snapdragon, 1000 MHz
- RAM: 576MB
- ROM: 512MB Flash
- WiFi: 802.11a/b/g/n
- Main Screen Resolution: 480 x 800
- 3G Network: GSM, CDMA

A. Working procedures

1) The user terminal which uses the 3G network or a WiFI network, checks whether it can connect to the 3G network or not. After checking, it sends the value of 3G networks in order to receive certificate from HTTPS sites (such as. Gmail.com).

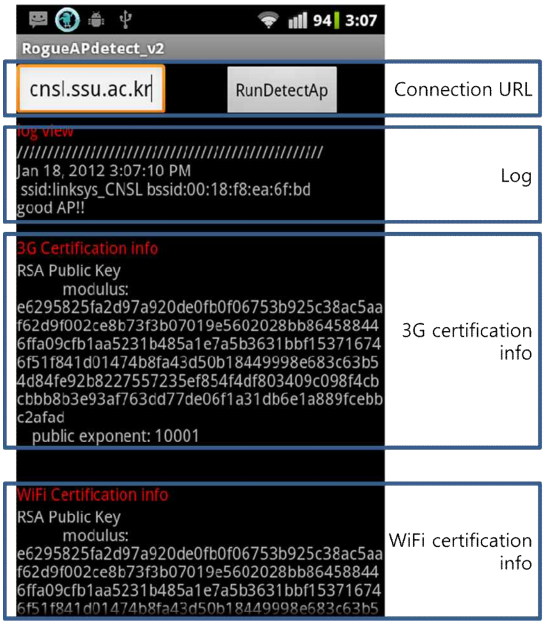
2) The certificate value that received by 3G network will be stored and will be used as a cache when the 3G network is used to access to same site again, thus reduce unnecessary operation.

3) WiFi interface is activated and connect to available AP's. After that a request is sent to the same HTTPs site to receive authentication value. Those authentication value will be stored in memory in order to compare the two certificates.

4) The authentication value transmitted though 3G networks are used for verification with the values sent via WiFi network. Certificate value is sent in hexadecimal, so the site certificate values can be seen through a string comparison. If there is any different of authentication value between WiFi network and 3G network, it will be considered as man-in-the-middle attack, in this case, user can connect to other AP and redo the verification process. If two certificates are same, that mean AP is safe and secure.

B. Application GUI

The user application has been designed for easily detecting the man-in-the-middle attack. The user interface has been designed so that in order to verify the certificate in a website, user only need to enter website domain and click the search buttons. The authentication value received from both 3G and WiFi networks are shown in Log screen. Log screen includes operating hours, SSID of current connection AP, BSSID and warning message if there is a man-in-the-middle attack occurs. Application GUI is illustrated by Figure 6 below:



```
cnsl.ssu.ac.kr

log view
//////////////////////////////////////////////////
Jan 18, 2012 3:07:10 PM
 ssid:linksys_CNSL bssid:00:18:f8:ea:6f:bd
good AP!!

3G Certification info
RSA Public Key
        modulus:
e6295825fa2d97a920de0fb0f06753b925c38ac5aa
f62d9f002ce8b73f3b07019e5602028bb86458844
6ffa09cfb1aa5231b485a1e7a5b3631bbf15371674
6f51f841d01474b8fa43d50b18449998e683c63b5
4d84fe92b8227557235ef854f4df803409c098f4cb
cbbb8b3e93af763dd77de06f1a31db6e1a889fcebb
c2afad
   public exponent: 10001

WiFi Certification info
RSA Public Key
        modulus:
e6295825fa2d97a920de0fb0f06753b925c38ac5aa
f62d9f002ce8b73f3b07019e5602028bb86458844
6ffa09cfb1aa5231b485a1e7a5b3631bbf15371674
6f51f841d01474b8fa43d50b18449998e683c63b5
```

Figure 6 Application GUI

V. Experiments and Results

In this paper, we design the environment where MITM occurs in order to test the effective of our scheme. We use Backtrack 5 OS to implement the MITM attack. The webmitm uses for fake certificate generation and ssldump is used for checking the log. We also created a wireless AP with airmon-ng and airbase-ng.

In order to create rogue AP, the following steps are implemented:

Firstly, airmon-ng is run for creating new wireless AP.

```
airmon-ng start wlan0
airbase-ng –c 6 –e "SSID" mon0&
```

Copyright (c) IARIA, 2012. ISBN: 978-1-61208-204-2

After that, we configure iptables, create air-interface, setting DHCP server and set https port forward.

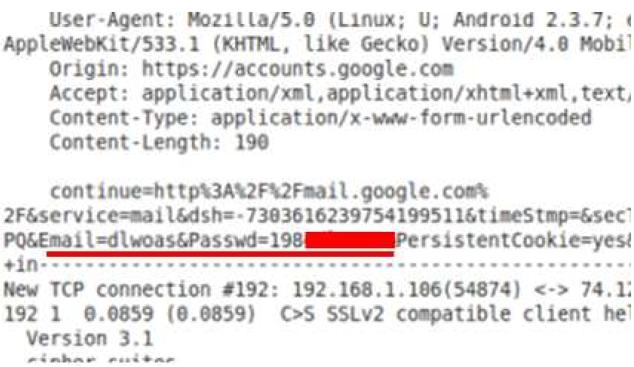
```
 #Clear out iptables
    iptables --flush
    iptables --table nat --flush
    iptables --delete-chain
 #Create a simple masquerade rule, routing all data of wlan1
    iptables --table nat --delete-chain
    iptables --table nat --append POSTROUTING --out-interface wlan2 -j
MASQUERADE
 #Accept anything coming in interface at0
    iptables --append FORWARD --in-interface at0 -j ACCEPT

 #Make sure forwarding is enabled
    echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
    ifconfig at0 up
    ifconfig at0 192.168.0.254 netmask 255.255.255.0
    route add -net 192.168.0.0 netmask 255.255.255.0 gw 192.168.0.254
    /etc/init.d/dhcp3-server start
    dhcpd3 -cf /etc/dhcp3/dhcpd.conf -pf /var/run/dhcp3-server/dhcpd.pid
at0

    iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT
    iptables -A FORWARD -j ACCEPT

    iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT
    iptables -A FORWARD -j ACCEPT
```

Next step, we run webmitm tool so that we can change the certificate, and ssldump for saving user information on log.txt

```
    webmitm –d
    ssldump –i at0 –n –d –k webmitm.crt | tee log.txt
```

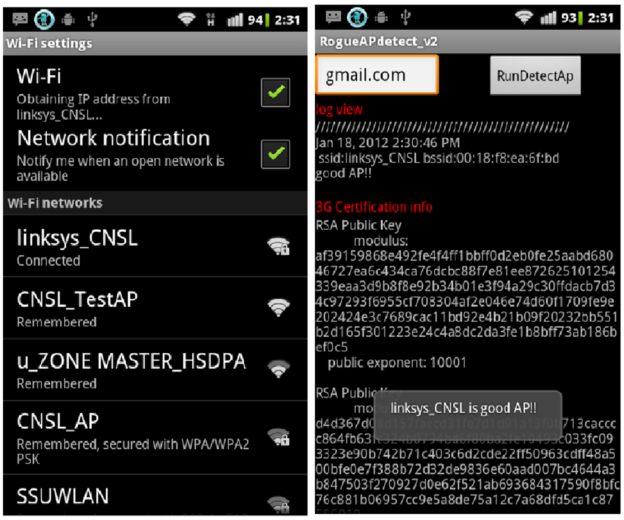
Result of MITM attack experiment has shown user's id and password even under secure environment (like gmail). Figure 7 illustrates the result of our MITM attack.



```
    User-Agent: Mozilla/5.0 (Linux; U; Android 2.3.7; 
AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobi
    Origin: https://accounts.google.com
    Accept: application/xml,application/xhtml+xml,text,
    Content-Type: application/x-www-form-urlencoded
    Content-Length: 190

    continue=http%3A%2F%2Fmail.google.com%
2F&service=mail&dsh=-7303616239754199511&timeStmp=&sec
PQ&Email=dlwoas&Passwd=198[redacted]PersistentCookie=yes
+in-----------------------------------------------------
New TCP connection #192: 192.168.1.106(54874) <-> 74.1
192 1  0.0859 (0.0859)  C>S SSLv2 compatible client he
  Version 3.1
```

Figure 7 Result of the attack

From the result of MITM attack, we can prove that MITM attack is possible and attacker can get user information from secure website. We also implemented our detection scheme against Man-in-the-middle attacks. Figure 8 and Figure 9 illustrate two results between normal AP and rogue AP situations. Figure 8 shows result when user connects to a normal AP "linksys_CNSL" and Figure 9 illustrates result with rouge AP "CNSL_TestAP" situation. The experimental results are as follows: In normal AP situation, the certified values transmitted via WiFi and 3G are the same. On the other hand, the authentication values are different in the AP "CNSL_TestAP" which is the man-in-the-middle.



Wi-Fi settings

Wi-Fi ☑
Obtaining IP address from linksys_CNSL...

Network notification ☑
Notify me when an open network is available

Wi-Fi networks

linksys_CNSL
Connected

CNSL_TestAP
Remembered

u_ZONE MASTER_HSDPA
Remembered

CNSL_AP
Remembered, secured with WPA/WPA2 PSK

SSUWLAN

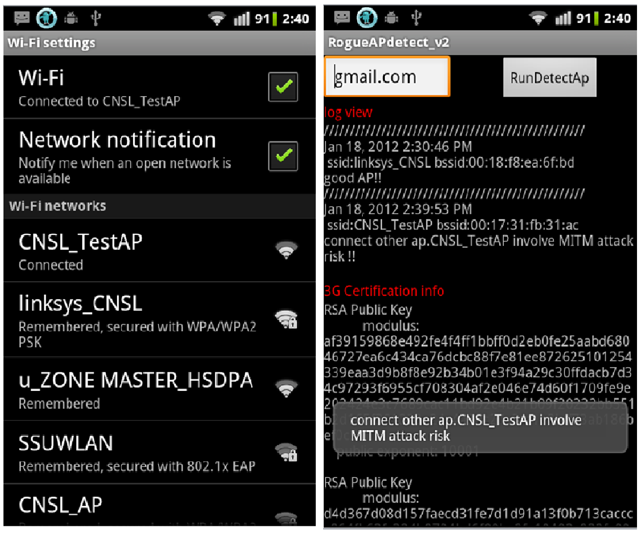
RogueAPdetect_v2

gmail.com | RunDetectAp

```
log view
///////////////////////////////////////////////////////
Jan 18, 2012 2:30:46 PM
 ssid:linksys_CNSL bssid:00:18:f8:ea:6f:bd
good AP!!

3G Certification info
RSA Public Key
        modulus:
af39159868e492fe4f4ff1bbff0d2eb0fe25aabd680
46727ea6c434ca76dcbc88f7e81ee872625101254
339eaa3d9b8f8e92b34b01e3f94a29c30ffdacb7d3
4c97293f6955cf708304af2e046e74d60f1709fe9e
202424e3c7689cac11bd92e4b21b09f20232bb551
b2d165f301223e24c4a8dc2da3fe1b8bff73ab186b
ef0c5
   public exponent: 10001

RSA Public
        mo
d4d367d0                                 713caccc
c864fb63                                 c033fc09
3323e90b742b71c403c6d2cde22ff50963cdff48a5
00bfe0e7f388b72d32de9836e60aad007bc4644a3
b847503f270927d0e62f521ab693684317590f8bfc
76c881b06957cc9e5a8de75a12c7a68dfd5ca1c87
```

linksys_CNSL is good AP!!

Figure 8 Result of the normal AP situation.



Wi-Fi settings

Wi-Fi ☑
Connected to CNSL_TestAP

Network notification ☑
Notify me when an open network is available

Wi-Fi networks

CNSL_TestAP
Connected

linksys_CNSL
Remembered, secured with WPA/WPA2 PSK

u_ZONE MASTER_HSDPA
Remembered

SSUWLAN
Remembered, secured with 802.1x EAP

CNSL_AP

RogueAPdetect_v2

gmail.com | RunDetectAp

```
log view
///////////////////////////////////////////////////////
Jan 18, 2012 2:30:46 PM
 ssid:linksys_CNSL bssid:00:18:f8:ea:6f:bd
good AP!!
///////////////////////////////////////////////////////
Jan 18, 2012 2:39:53 PM
 ssid:CNSL_TestAP bssid:00:17:31:fb:31:ac
connect other ap.CNSL_TestAP involve MITM attack
risk !!

3G Certification info
RSA Public Key
        modulus:
af39159868e492fe4f4ff1bbff0d2eb0fe25aabd680
46727ea6c434ca76dcbc88f7e81ee872625101254
339eaa3d9b8f8e92b34b01e3f94a29c30ffdacb7d3
4c97293f6955cf708304af2e046e74d60f1709fe9e
2                                        1
b                                        b
e

RSA Public Key
        modulus:
d4d367d08d157faecd31fe7d1d91a13f0b713caccc
```

connect other ap.CNSL_TestAP involve MITM attack risk

Figure 9 Result of the MITM attack situation

VI. A COMPARISON OF DEFENSE TECHNIQUES

MITM attack detection techniques have already been proposed through the use of additional equipment or the use of wireless sensors. Another approach like radius authentication server which uses a wired or wireless network with prevention techniques and detection methods that are managed by the operator to detect man-in-the-middle attack techniques in same network also need separate equipment required to install and operate, and must be regularly monitored by the administrator. Table II shows the comparison between various defense techniques

TABLE II. A COMPARISON TABLE OF DEFENSE TECHNIQUES

Techniques	**Cost**	**Features**	**Requirements**
Detect rogues AP with sensor	High cost to install a wide range	Detect man-in-the-middle attacks by analyzing packets	Requires a large number of sensors
Rogue AP Protection System Based On Radius Authentication Server	High cost to installation and maintenance costs	Radius authentication server can communicate with the AP through a secure	Difficulties detect rogue AP on open environment
Detection technique using wired and wireless networks	High cost to installation and maintenance costs	Get information from wired and wireless network	Difficulties detect rogue AP on open environment
Detect rogue AP Using 3G network	None	User terminal can be detected n the man-in-the-middle attacks	Install application

However, the proposed technique without modification to an existing protocol from the user terminal and no additional equipment needed, is available in any location and environment, man-in-the-middle attacks can be detected directly from your handset, so users can apply in every situation, because what they are compared to existing techniques it can be called a practical and effective.

VII. CONCLUSIONS

As the WiFi smart phone users increase, security threats also increase. To protect user privacy at the Web server, a secure SSL authentication technique is applied against man-in-the-middle attacks, but the risk of hacking still exists. To prevent this attack, many techniques and services have been proposed to be applied to all users, but the implementation cost is a limit. Proposed scheme is very simple and effective for detecting man-in-the-middle attacks because it does not require huge implementation cost or expensive security sensors. The other advantage of our system is that users can directly determine man-in-the-middle attack at any time and any place. Our scheme does not need any modification in current protocol or developing a new protocol, so it is a practical and effective technique. The disadvantage of proposed method is that it can only detect an attack which attempts to modify the certificate. We will further study other types of attacks to make our solution to be more applicable.

ACKNOWLEDGMENT

“This research was supported by the KCC (Korea Communications Commission), Korea, under the R&D program supervised by the KCA (Korea Communications Agency)” (KCA-2012- 08-911-05-001)

REFERENCES

[1] K. Cheng, M. Gao, and R. Guo, "Analysis and Research on HTTPS Hijacking Attacks," 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, IEEE, pp. 223-226, Apr. 2010.

[2] M. Moixe, "New Tricks For Defeating SSL in Practice", BlackHat Conference, USA. Feb. 2009.

[3] T. Koutny, "Detecting Unauthorized Modification of HTTP Communication with Steganography," 2010 Fifth International Conference on Internet and Web Applications and Services, IEEE, pp. 26-31, May. 2010.

[4] Internet Incident Response Support Center, ” Internet Attack Trends and Analysis,” Korea Information Security Agency, pp. 22-37, Jun. 2007

[5] D. Jiang, L. Xinghui, and H. Hua, "A Study of Man-in-the-Middle Attack Based on SSL Certificate Interaction," 2011 First International Conference on Instrumentation, Measurement, Computer, Communication and Control, pp. 445-448, Oct. 2011.

[6] F. Callegati, W. Cerroni, and M. Ramilli,, "Man-in-the-Middle Attack to the HTTPS Protocol," Security & Privacy, IEEE, pp. 78-81, 2009.

[7] R. Meyer, "Secure Authentication on the Internet, " SANS InfoSec Reading Room - Securing Code, Feb. 2008.

[8] S. Yimin, Y. Chao, and G. Guofei, "Who Is Peeping at Your Passwords at Starbucks? - To Catch an Evil Twin Access Point," International Conference on Dependable Systems & Networks (DSN), IEEE, June. 2010.

[9] T. Chomsiri, ”HTTPS Hacking Protection, ” 21st International Conference on Advanced Information Networking and Applications Workshops, IEEE, May. 2007.

[10] K. kuofong, L .ien, and L. Yuehchia, "Detecting rogue access points using client-side bottleneck bandwidth analysis," Computers & Security, vol. 24(3-4), ELSEVIER, pp. 144-152, May. 2009.

[11] L. Watkins, R. Beyah, C. Corbett, "A Passive Approach to Rogue Access Point Detection," Global Telecommunications Conference, 2007. IEEE. pp. 355-360, Nov.2007

[12] K. DongPhil, K. chulbum, and K. Sangwook, “Rogue AP Protection System Based On Radius Authentication Server,” Korean Institute of Information Scientists and Engineers, vol. 31(1), April, 2004.

[13] 3GPP TS 33.102, “3G security; Security architecture,” 3GPP, Rel-11, version11.1.0, Dec. 2012.

[14] K. Kuofong, Y.Taoheng, Y.waishuoen, and C.Huihsuan, "A location-aware rogue AP detection system based on wireless packet sniffing of sensor APs," SAC '11 Proceedings of the 2011 ACM Symposium on Applied Computing, ACM, 2011.

[15] B. Yan, G. Chen, J. Wang, and H. Yin, "Robust Detection of Unauthorized Wireless Access Points," Mobile Networks and Applications Journal, vol. 14(4), pp. 508-522, Aug. 2009.

[16] R. Beyah, "Rogue access point detection_challenges, solutions, and future directions," IEEE Security and Privacy Article, vol. 9(5), IEEE, pp. 56-61, 2011.