

Security Enhanced IEEE 802.1x Authentication Method for WLAN Mobile Router

Keun Young Park*, Yong Soo Kim*, Juho Kim*

* Department of Computer Science & Engineering, Sogang University, Seoul, Korea

kypark@sogang.ac.kr, kimmool@sogang.ac.kr, jhkim@sogang.ac.kr

Abstract—Along with the diffusion of smart devices that use WLAN, the number of WLAN Hotspot is rapidly increasing. A representative security threat in WLAN environments is hacking using rogue APs (Access Point). To prevent this security threat, the WLAN security standard applies the IEEE 802.1x authentication method. In this authentication method, RADIUS servers authenticate APs using static shared secrets. However, this method is not suitable for WLAN environments where mobile routers are used. Mobile routers are always exposed to device hacking and thus they are subject to very high risks of the leak of shared secrets. Therefore, they require securer authentication methods. In this paper, a new IEEE 802.1x based authentication method of which the security has been enhanced using TPMs (Trusted Platform Module) is proposed. Unlike existing methods, the proposed method involves no risk of authentication key leaks at all and can fundamentally block any attempt of hacking using rogue APs as the server verifies the integrity of APs in the process of authentication.

Keywords—WLAN, Access Point, IEEE 802.1x Authentication, TPM, Mobile Router

I. INTRODUCTION

Thanks to the development of WLAN technology and the expansion of infrastructures, an age has come where the Internet can be accessed anytime anywhere using WLAN. In particular, since WLAN Hotspots are established using 3G/4G Mobile Routers, it has become possible to use WLAN even in running buses or subways. By using a Mobile Router, a WLAN Hotspot can be established at a relatively low cost regardless of places. Therefore, it is expected that the use of Mobile Routers as WLAN APs will greatly increase in LTE or LTE-A based next generation communication environments.

A representative security threat in WLAN environments is MITM (Man-in-the-middle) attacks using rogue APs. In these attacks, as shown in Figure 1, the attacker lures the user using an AP (Access Point) installed with a hacking tool and then intervenes in the middle of communication processes to tap or falsify the contents of communication while providing WLAN services [1]. To block these attacks, IEEE 802.11i, a WLAN security standard applies the IEEE 802.1x authentication

method where RADIUS servers are used [2][3]. This security method supports diverse EAP (Extensible Authentication Protocol) based authentication protocols to provide diverse mutual authentication methods between the AP and the user device [4]. However, in WLAN environments configured using mobile routers; it is difficult to ensure sufficient security in the existing IEEE 802.1x authentication method. In the existing 802.1x authentication method, RADIUS servers authenticate each AP using only the static shared secret possessed by the AP and the MAC address of the AP is additionally used in some types of authentication. This method is effective in existing WLAN environments where APs are subordinate to LAN. However, the existing method that uses static shared secrets cannot provide a sufficient level of security in mobile router environments since APs are mobile and always exposed to hacking in these environments. If an attacker hacks into the mobile router in service to obtain the shared secret and MAC address, the attacker will be able to easily configure the rogue AP using these two pieces of information and attempt MITM attacks from anywhere. Therefore, mobile routers require security methods that have been strengthened further compared to existing IEEE 802.1x.

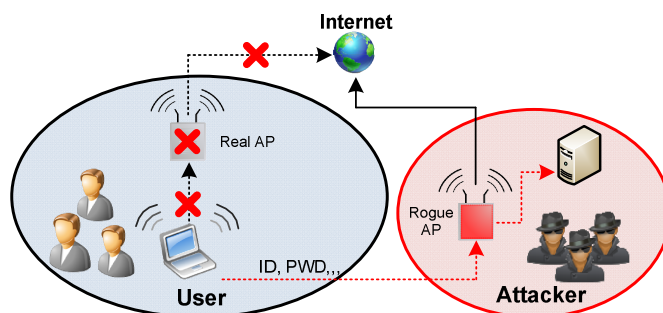


Figure 1. Man in the middle attack using rogue access point

In this paper, the vulnerability of the existing IEEE 802.1x authentication method in WLAN environments configured using mobile routers is demonstrated and an IEEE 802.1x based authentication method with enhanced security is proposed. The proposed method enables RADIUS servers to check the integrity and authenticity of each AP using the RTR

(Root of Trust for Reporting) function of TPM to fundamentally block MITM attacks using rogue APs.

This paper is composed as follows. In Chapter2, the vulnerability of the existing IEEE 802.1x authentication method and TPM are described and in Chapter 3, the proposed method is described. In Chapter 4, the security of the proposed method is analysed and in Chapter 5, the experimental results are shown. In Chapter 6, conclusions are formed

II. RELATED WORKS

A. Research on IEEE 802.1x security technology

IEEE 802.11i, a WLAN security standard employed IEEE 802.1x as a large frame for WLAN system user authentication and key exchanges and defined it as an essential item to be implemented for security. IEEE 802.1x defines port based access control functions and supports diverse TLS based EAP mutual authentication protocols. Therefore, it enables mutual authentication between the AP and the user device thereby providing a means to block MITM attacks using rogue APs.

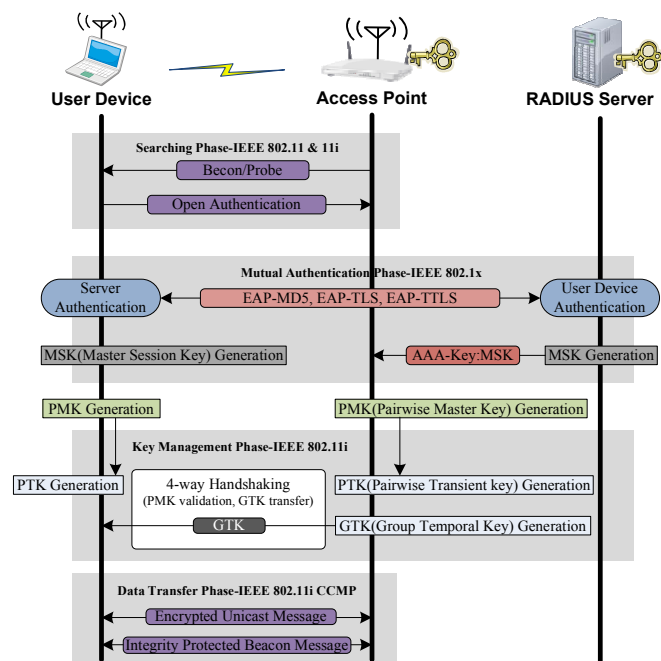


Figure 2. WLAN security procedure based on IEEE 802.11i & IEEE 802.1x

Figure 2 shows a device that uses IEEE 802.1x in IEEE 802.11i and the procedure for mutual authentication between the device and an AP. In the IEEE 802.11i security standard, IEEE 802.1x largely serves the roles of conducting user authentication and delivering MSKs (Master Session Key) generated in the process of the authentication to be used for wireless MAC layer security to APs. This procedure is as follows. First, in the Mutual Authentication Phase shown in Figure 2, mutual authentication between the wireless device and the RADIUS server is performed through a TLS based EAP authentication protocol such as EAP-MD5, EAP-TLS or EAP-TTLS. Then, the user device and the server create a MSK necessary for the encryption of wireless links between

the user device and an AP using the TMS (TLS Master Secret) shared in the process of authentication.

Now, the server delivers the created MSK to the AP. The AP does not know the MSK because the AP is not an end point of the EAP authentication protocol. The server delivers the generated MSK to the AP using a RADIUS packet. At this time, the MSK is encrypted using the shared secret between the AP and the server. Thereafter, the user device and the AP generate a PMK (Pairwise Master Key) using the MSK. Then, the user device verifies if the AP has the same PMK as the one owned by the user device through a key management procedure specified as a 4-way handshake procedure using EAPoL-Key frames with the AP to authenticate the AP. When all the verification procedures have been completed, the user device encrypts data frames on wireless links using key sets generated using the PMK.

B. Security problems of IEEE 802.1x authentication method in WLAN using mobile router

In the mutual authentication phase of the IEEE 802.11i security procedure, the user device and the server authenticate each other using an EAP based authentication protocol. On the other hand, the user device and the AP mutually authenticate in the key management phase. In this process, the user device and the AP check each other if the other party has the same PMK as the one owned by him through a 4-way handshake to authenticate the party. In the IEEE 802.11i security procedure, the user device and the AP generate a PMK using the MSK generated through a key exchange procedure between user device and the server in the mutual authentication phase. When the server delivers the MSK to an AP, the server encrypts the MSK using the shared secret with the AP as a key. Therefore, when seen from the standpoint of the user device, if the AP had the same PMK as possessed by it, that means that the AP currently accessed by it is the real AP known by the server. Consequently, from the standpoint of the user device, AP authentication can be said to be a process through which the user device checks whether the AP knows the shared secret.

The existing authentication method applied to IEEE 802.1x that uses shared secrets between APs and servers is a relatively safe method in WLAN environments configured with LAN based APs. In these environments, APs are fixed to certain positions and thus physical security may be expected depending on environments where APs are installed and MAC address based additional access controls may be applied using LAN switches, etc.. However, in WLAN environments where mobile routers are used, the existing IEEE 802.1x authentication method cannot provide a sufficiently high level of security any further. Mobile routers are mobile and portable and physical security for them cannot be expected and they are always exposed to the risks of robbery and device hacking. Furthermore, shared keys exist as plaintexts in APs' configuration files. Therefore, if an attacker obtains a mobile router currently in service and finds out the router's shared secret with the server through device hacking mobilizing reverse engineering, the attacker will become able to easily configure rogue APs with the mobile router owned by him

using the information. Therefore, for WLAN environments where mobile routers are used, authentication methods should be equipped with the following two security requirements.

- Req.1: Even if an attacker hacks an AP, the attacker should not be able to find out the shared key and MSK used for authentication.
- Req.2: Even if a device is hacked, it should not affect the safety of the authentication system or other devices.

C. Trusted Platform Module

A TPM is a secure crypto processor composed of an independent chipset. As shown in Figure 3, each TPM is equipped with not only a Random Number Generator and a Hash engine but also a RSA key generator, a key storage, and an RSA engine [5].

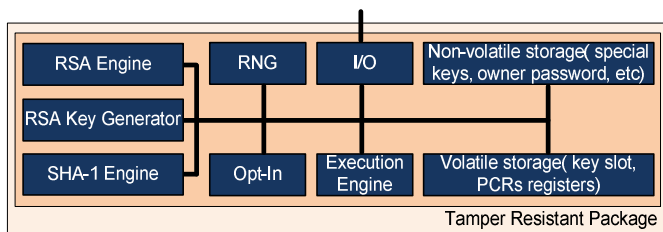


Figure 3. Architecture of Trusted Platform Module

All TPMs have a 2048-bit RSA asymmetric key pair called Endorsement Key (EK). Each EK is unique to each TPM. It is generated chipset manufacturing time and cannot be changed. Furthermore, each EK's private key exists in the TPM only and thus cannot be analysed at all and public keys are safely distributed through certificates signed by the CA or the manufacturer.

Major functions of TPMs include RTM (Root of Trust for Measurement) and RTR (Root of Trust for Report). The RTM is a process for a TPM to verify the integrity of software in each device where the Hash values of software currently being executed are calculated and the results are accumulated in PCRs(Platform Configuration Registers) in the TPM. The RTR is a function to report system conditions to third parties by signing on the values of PCRs generated in the process of RTMs with private key in TPMs and sending the values to third parties. For RTRs, TPMs generate and use RSA key pairs called AIK (Attestation Identity Keys).

III. PROPOSED METHOD

A. Overview of proposed authentication method

Unlike the existing IEEE 802.1x authentication method, the method proposed in this paper does not use the static shared secret in authentication between RADIUS servers and APs but applies a new device authentication method using TPM. The proposed method has been enabled to authenticate APs of which the access is requested by the server using the EK and RTR function of TPM as well as verifying the integrity of the APs. Furthermore, it has been made to encrypt MSK generated through mutual authentication between the user device and the server using a public key of the TPM when the

MSK are delivered to the AP so that the MSK can be decrypted using only the TPM. For the aforementioned features, the proposed method has the following preconditions for APs and servers.

- Access Point: All APs are assumed to have been equipped with a TPM. Each TPM has a unique EK and the certification of the EK issued by the manufacturer of the TPM or APs.
- RADIUS Server: The server has AP Serial Number (SN) and EK lists stored in its database along with information for user authentication. It also has default PCRs values for individual AP models and software versions in its database.

In the proposed method, only those APs that have been registered in the server in advance can be authenticated by the server to provide WLAN services. Therefore, all APs should be registered with the server through specified procedures. The proposed method is composed of a process to register APs to servers and an IEEE 802.1x based authentication process using registered APs.

B. Access Point initialization & registration procedure

In the proposed method, for a WLAN AP to be authenticated by a RADIUS server, the AIK of the TPM should be registered and then the certificate of the AIK should be registered with the server. This process is as shown in Figure 4.

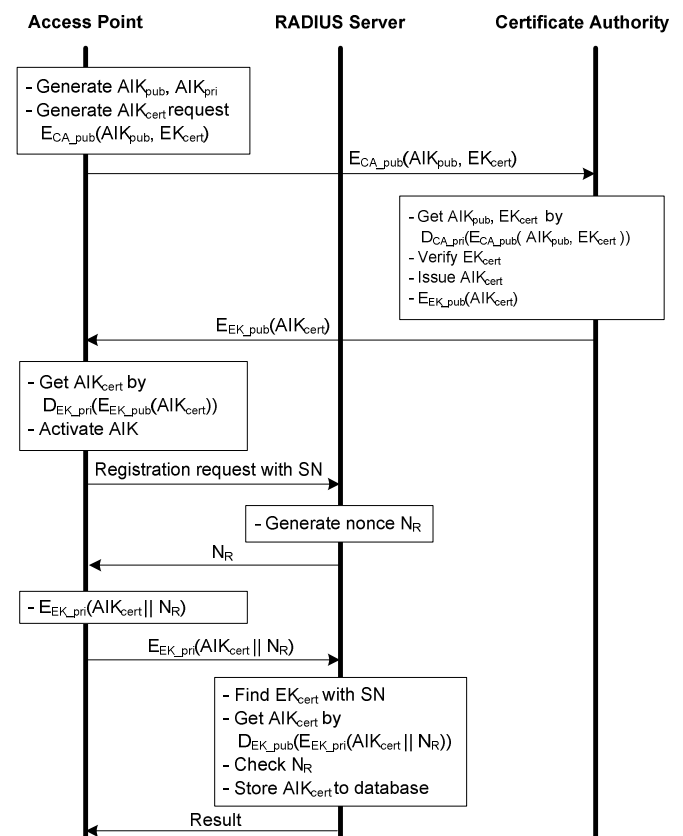


Figure 4. Access Point initialization & registration procedure

An AP initializes its TPM and generates an AIK asymmetric key pair. Then, it requests the CA (Certificate Authority) to issue a certificate for the generated AIK. In this case, the AIK_{pub} , the public key of the AIK and the EK_{cert} , the certificate of the TPM are encrypted with the CA_{pub} , the public key of the CA and the result, $E_{CA_{pub}}(AIK_{pub}, EK_{cert})$ is transmitted to the CA to request for the issuance of the certificate. Then, the CA verifies the message transmitted by the AP requesting for the issuance of the certificate and issues AIK_{cert} , the certificate of the AIK. First, the CA decrypts the request from the AP using its private key, CA_{pri} to obtain AIK_{pub} and EK_{cert} . Then, the CA verifies EK_{cert} and issues an AIK_{cert} that includes the AIK_{pub} and was signed by its private key. Then, the CA encrypts the issued AIK_{cert} with the public key of the TPM included in the EK_{cert} and deliver to the AP.

Finally, the AP checks the AIK_{cert} generated by the CA and registers the AIK_{cert} with the RADIUS server. First, the AP decrypts the $E_{EK_{pub}}(AIK_{cert})$ delivered by the CA using EK_{pri} , its private key to obtain the AIK_{cert} issued by the CA. Then, it sends an AIK registration request to the server along with an SN and obtains a random nonce N_R generated by the server. Then, it encrypts the AIK_{cert} and the N_R using the EK_{pri} to obtain an $E_{EK_{pri}}(AIK_{cert}||N_R)$ and transmits it to the server to request for registration. Now, the server finds out the EK_{cert} of the AP using the SN transmitted by the AP and then decrypts the message transmitted by the EK_{pub} AP to obtain the AIK_{cert} and the N_R . If the obtained N_R is the same as the value generated by it, the server stores the AIK_{cert} in its database and finishes the registration procedure.

C. IEEE 802.1x authentication procedure

The proposed IEEE 802.1x authenticate method is as shown in Figure 5. It is assumed that the WLAN AP has been already registered with the RADIUS server.

After the initial wireless access procedure between the user device and the AP, the AP should prove its integrity to the server to be authenticated before a mutual authentication phase between the user device and the server begins. This process is as follows. First, the AP sends an SN to the server to request for access. Then, the server checks the SN transmitted by the AP, generates a random nonce N_A and transmits it to the AP to request for device attestation. Now, on receipt of the request, the AP generates an attestation value using its TPM. The TPM concatenates the PCR's values generated in the device boot procedure with the N_A , signs on the result using its AIK_{pri} to obtain an attestation value and transmits the value to the server. Now, the server verifies the attestation value delivered by the AP to authenticate the AP. First, the server loads the AIK_{cert} of the AP and the default PCR value PCR's' from its database using the SN. Then, the server decrypts the attestation value delivered by the AP using the AIK_{pub} and compares it with the PCR's' and N_A possessed by it to authenticate and verify the integrity of the AP device. Then, the server notifies the result to the AP.

When the Device authentication procedure has been completed, the user device and the server perform TLS based EAP mutual authentication and deliver the MSK generated through the authentication to the AP. In this case, the server

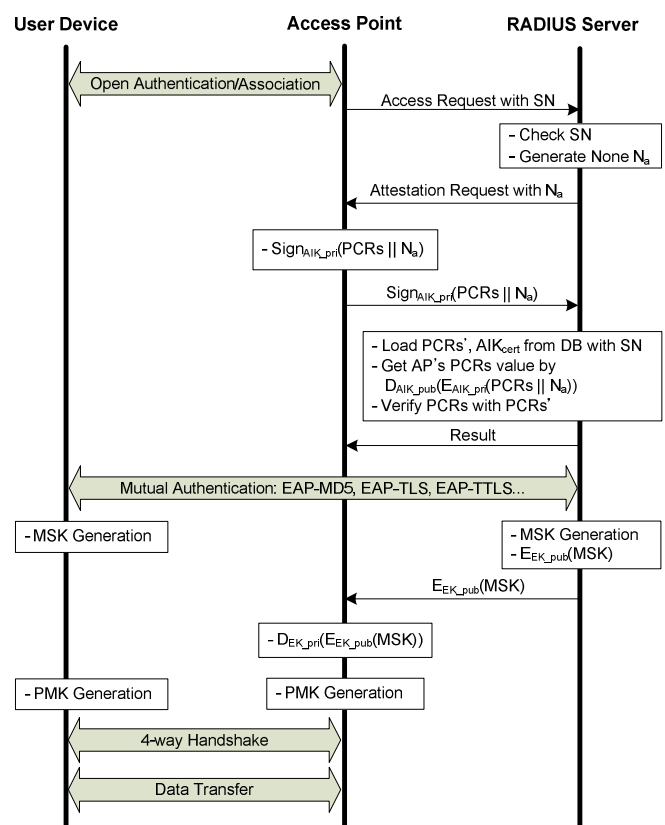


Figure 5. Security enhanced IEEE 802.1x authentication procedure

encrypts the MSK using the EK_{pub} , the TPM public key of the AP before delivering it. On receipt of it, the AP delivers the encrypted MSK to the TPM so that it is decrypted in the TPM using its EK_{pri} . When this process has been completed, the PMK generation and 4-way handshake processes as used in the existing method are undergone to perform authentication and key agreement between the user device and the AP and begin encrypted communication in the wireless link.

IV. SECURITY ANALYSIS

The method proposed in this paper provides a higher level of security compared to the existing IEEE 802.1x authentication method. In the proposed method, only those APs registered with the RADIUS server in advance and verified for integrity can provide WLAN services.

In the AP initialization & registration procedure, the server decrypts the $E_{EK_{pri}}(AIK_{cert}||N_R)$ delivered by the AP using the EK_{cert} corresponding to the SN and compared the N_R with the values generated by it. On the other hand, the key EK_{pri} used by the AP in the encryption exists only in the TPM and cannot be modified. Therefore, only those APs known by the server can register their AIK_{cert} .

In the authentication procedure of the proposed method, the server verifies the attestation value presented by the AP requesting for access to authenticate the AP. That is, the server compares the N_A obtained by decrypting the attestation value generated by the TPM of the AP with the N_A possessed

by it to see if they are the same to check whether the AP has been registered in advance and verifies the integrity of the AP by comparing PCR's values. This method provides a higher level of security compared to the existing method where anyone that knows the server's shared secret can be authenticated by the server. In addition, the proposed method encrypts the EK_{pub} of the TPM with a key in the process of delivering the MSK generated through mutual authentication between the user and the server to the AP. The EK_{pri} of the TPM exists only in the TPM. Therefore, the encrypted MSK can be decrypted by only those APs registered with the server. Therefore, this method provides a higher level of security compared to existing methods where anybody that knew shared secrets could decrypt MSK.

V. EXPERIMENT

The method proposed in this paper requires additional asymmetric key cryptographic operations for AIK_{cert} registration processes and AP authentication processes compared to the existing IEEE 802.1x authentication method. Furthermore, all these cryptographic operations on APs are performed by TPMs. Therefore, the size of the overhead of the proposed method is determined by the cryptographic operation time of TPMs.

TABLE 1. EXECUTION OVERHEAD OF CRYPTOGRAPHIC OPERATIONS OF PROPOSED METHOD ON ACCESS POINT (MS)

Phase	Key generation	(E)ncryption, (D)ecryption	PCR Read	PCR Sign
Registration	758.00	E.1: 594.23, D.1: 532.24, E.2: 561.68	0	0
Auth-entification	0	D.1: 556.34	46.01	511.44

Table 1 shows the results of measurements of the overheads for cryptographic operations on APs required in the process of implementing each phase of the proposed method. The experimental environment was implemented using TPM/J API [6] on Linux kernel ver.2.6.25.4 and the overheads were measured using ATMEL TPM Ver. 1.2, installed on Lenovo ThinkPad X60s(Intel Core Duo 1.6GHz, 1GB RAM). As shown in the experimental results, the time required to perform the cryptographic operations of the proposed method on a TPM is very short. Therefore, the effect of the proposed method on the authentication procedure of APs is not big.

VI. CONCLUSIONS

In this paper, a new IEEE 802.1x based authentication method with enhanced security was proposed. The proposed method applied the RTR function of TPMs to authentication procedures between APs and servers so that the integrity of the APs requesting access is verified. Furthermore, the method was made to authenticate APs using EKs, unique keys of TPMs to safely deliver MSKs generated through authentication to APs. Therefore, by applying the proposed method, MITM attacks using rogue APs can be fundamentally

blocked. However, the proposed method does not require any change in WLAN user devices. In addition, since TPMs provide most software toolkits necessary for its application even though they are cheap and thus the proposed method can be applied easily at low costs.

ACKNOWLEDGMENT

This study was conducted with the support of the Telecommunication R&D center of Samsung Electronics Co., Ltd.

REFERENCES

- [1] R. H. Rahman, N. N. Nowsheen, M. A. Khan and V. H. Khan, "Wireless Lan Security: An In-Depth Study of the Threat and Vulnerabilities," Asian Journal of Information Technology, vol. 6(4), pp.441-446, 2007.
- [2] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification Amendment 6: Medium Access Control (MAC) Security Enhancements*, IEEE Std. 802.11i, 2004.
- [3] *DRAFT Standard for Local and Metropolitan Area Networks-Port-Based Network Access Control (Revision)*, IEEE P802.1x-REV/D11, 2004.
- [4] K. M. Ali and T. J. Owens, "Selection of an EAP authentication method for a WLN," International Journal of Information and Computer Security, vol. 1(1), pp. 210-233, 2007
- [5] TPM Main Part 1 Design Principles: Specification version 1.2, Trusted Computing Group, 2011.
- [6] L. Sarmenta, J. Rhodes, T. Muller, "TPM/J Java-based API for the Trusted Platform Moudle (TPM)," MIT CSAIL, Available: <http://tpm-emulator.berlios.de/>, Nov. 25