Chapter 2

Related Works

A large number of network security researches and proposals have been proposed for wireless LANs recently. The IEEE organization introduced an end-to-end security framework, 802.1x standard, in 2001 to solve the weakness of IEEE 802.11 wireless LAN. Nowadays, this standard has become the most popular requirement in wireless devices. The IEEE 802.1x standard for port based network access control provides the authentication mechanism and an optional capability key management framework. However, the 802.1x security is still not sufficient for many people. The ultimate goal will be the IEEE 802.11i, a robust security. In this chapter, we will describe the IEEE 802.1x architecture, authentication, key management, and

a high profile type EAP-TLS [12]. In final, we give the IEEE 802.11i overview briefly.

2.1 IEEE 802.1x Architecture

The IEEE 802.1x defines three components, supplicant, authenticator, and authentication Server. We illustrate the IEEE 802.1x infrastructure in figure 2-1. The supplicant is the mobile station that the end user try to access the network. The authenticator is the AP that controls the network access incoming and outgoing packets. The authenticator actually performs such as a bridge between the supplicant and authentication server, but additionally it has to maintain the state machine from the exchange information during the 802.1x authentication phase. The packet is passed to the authentication server for actual authentication processing. Most practical cases are using the IETF standard "Remote authentication dial in user service (RADIUS)" [13] server as the authentication server.

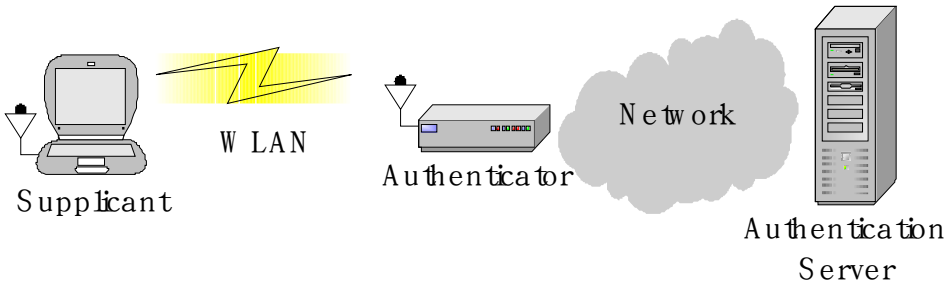

Figure 2-1. The IEEE 802.1x network infrastructure

The IEEE 802.1x uses an existing protocol, the Extensible Authentication Protocol (EAP) [14], that was initially developed in the Point-to-Point Protocol (PPP) [15]. The IETF standardizes the EAP encapsulation to enable it running over any link layer, such as PPP links, Ethernet, token ring, or even wireless LANs.

2.2 IEEE 802.1x Authentication

The IEEE 802.1x, known as Port-Based Network Access Control, provides an authentication framework in the wireless LANs. It uses a dual-port model concept, uncontrolled port and controlled port. It assumes that the authenticator has two ports of access to the network. Figure 2-2 shows the switch of port control. The uncontrolled port blocks all the network traffic, except the EAP packets. Those packets coming from an unauthorized supplicant are allowed through the

uncontrolled port. In the other words, the unauthorized supplicant is only allowed to send the authentication packet, within EAP-encapsulation, through the authenticator.

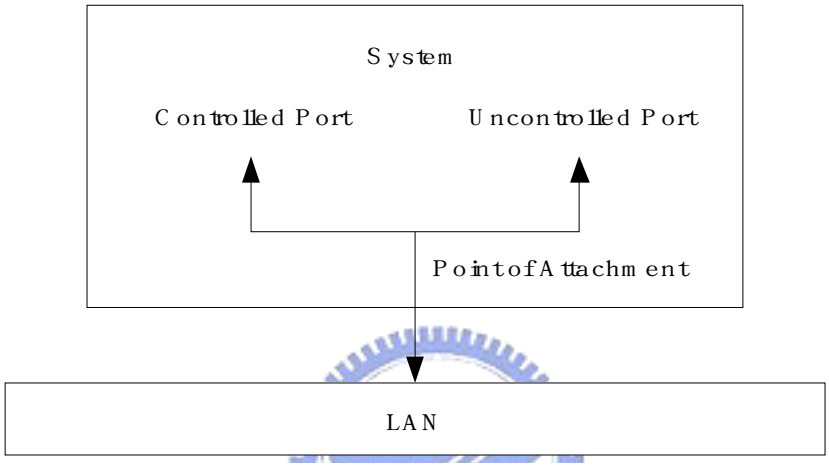

Figure 2-2. The controlled and uncontrolled port of the authenticator

Before the EAPOL exchanges, the supplicant and authenticator must be able to communicate by each other, thus they have to finish the conventional IEEE 802.11 authorized process, authentication and association states. Note that the authentication of 802.11 will use the Open-System Authentication (OSA) type to allow the following association request.

The authentication procedure of 802.1x is stated as follows (see figure 2-3):

1. When the association is completed, the supplicant issues the EAPOL-Start request to trigger the EAP exchange.

2. The authenticator sends the EAP-Request/Identity frame to the supplicant.

3. The supplicant replies the EAP-Response/Identity frame that is passed to the RADIUS server as a Radius-Access-Request.

4. The RADIUS server sends a Radius-Access-Challenge frame that passed to the supplicant as EAP-Request for validation.

5. The supplicant replies the challenge with an EAP-Response, which is translated by the authenticator into a Radius-Access-Request.

6. Finally, the RADIUS server permits the request and tells the authenticator with Radius-Access-Accept packet. The authenticator issues an EAP-Success packet for supplicant. In the meantime, the port is opened, and the supplicant can start accessing the network.

When the supplicant is going to leave the network, it can issue EAPOL-Logoff frame to de-authorize the port.

Figure 2-3. The IEEE 802.1x network with EAPOL exchange

2.3 IEEE 802.1x Key Management

IEEE 802.1x provides an optional capability of key management. It uses EAPOL-Key frame to send the secret key from the access point to the station. The EAPOL-Key, key exchange frame, is only sent after the authentication success, and irrespective of the authentication method used (EAP-TLS, EAP-MD5 [16]). Figure 2-3 shows the key distribution "EAPOL-Key" frame in 802.11 wireless LANs.

This key distribution is also called "Broadcast Key Rotation" (BKR). In this technique, the access point can actively broadcast the WEP key periodically, stations create the session encryption key by combining the Initialization Vector (IV) with the broadcast WEP key as well. In general, the broadcast period is a configurable variable and can be set by the administrator.

Although the 802.1x solves a lot of security problems in the current wireless network, but it involves infrastructural change. That is, the access point and stations hardware need to be changed and upgraded.

2.4 EAP-TLS Authentication Protocol

As described before, the 802.1x is based on EAP protocol. There are several authentication methods, such as MD-5 [17] challenge, One-Time Password (OTP) [18], and Transport Layer Security (TLS) [19] allowed in EAP protocol. Among these methods, TLS is one of the most popular methods. In this section we will give a brief introduction of EAP-TLS.

The TLS is derived and standardized from the Secure Socket Layer (SSL). On the Internet, the TLS authentication protocol is usually performed over Transmission Control Protocol (TCP). But in EAP-TLS, the TLS is processed over EAP protocol. Irrespective of underlying protocol, TLS takes advantage of the mutual authentication and key exchange. That is, not only the server can authenticate the client, but the client can also ensure that is connecting to a legitimate server. Besides, both client and server exchange key by each other during authentication, this provides a mechanism for session key establishment.

We illustrate the EAP-TLS exchanges in figure 2-4. The RADIUS server issues an “EAP-TLS Start” packet to begin the negotiation, the supplicant replies the “TLS client_hello” packet as EAP-Response. Then the RADIUS server sends the “TLS server_hello” packet as EAP-Request. It contains the RADIUS server

certificate and requests the certificate of supplicant. The supplicant validates the RADIUS server certificate and replies its certificate and cryptography specification in EAP-Response frame. Finally, the supplicant is validated, the RADIUS server sends an EAP-Request with cryptography specification for this session.

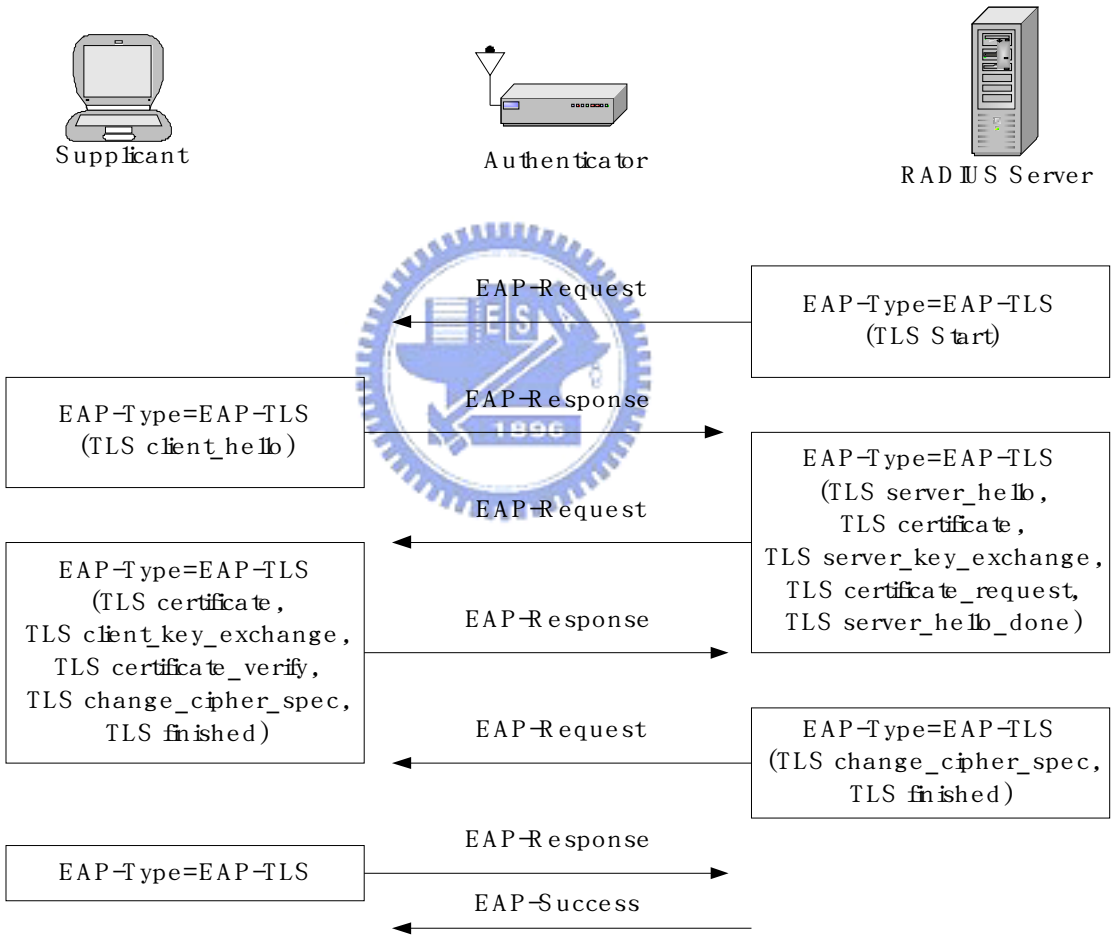

Figure 2-4. The EAP-TLS mutual authentication protocol

Both supplicant and RADIUS server derive the session keys independently at the end of EAP-TLS authentication. The session keys, showed in figure 2-5, are based on the master secret, thus we have to generate the master secret in first. The random value, pre-master secret, and "master secret" string value are computed by the pseudo-random function (PRF) to generate the master secret. The PRF is defined in the TLS specification, the random value is the concatenation of the exchange message fields client_hello.random and server_hello.random, and the pre-master secret sent from supplicant to RADIUS server is encrypted by server's public key. The PRF is used again to generate the session keys along with random value, master secret, and "client EAP encryption" string value.

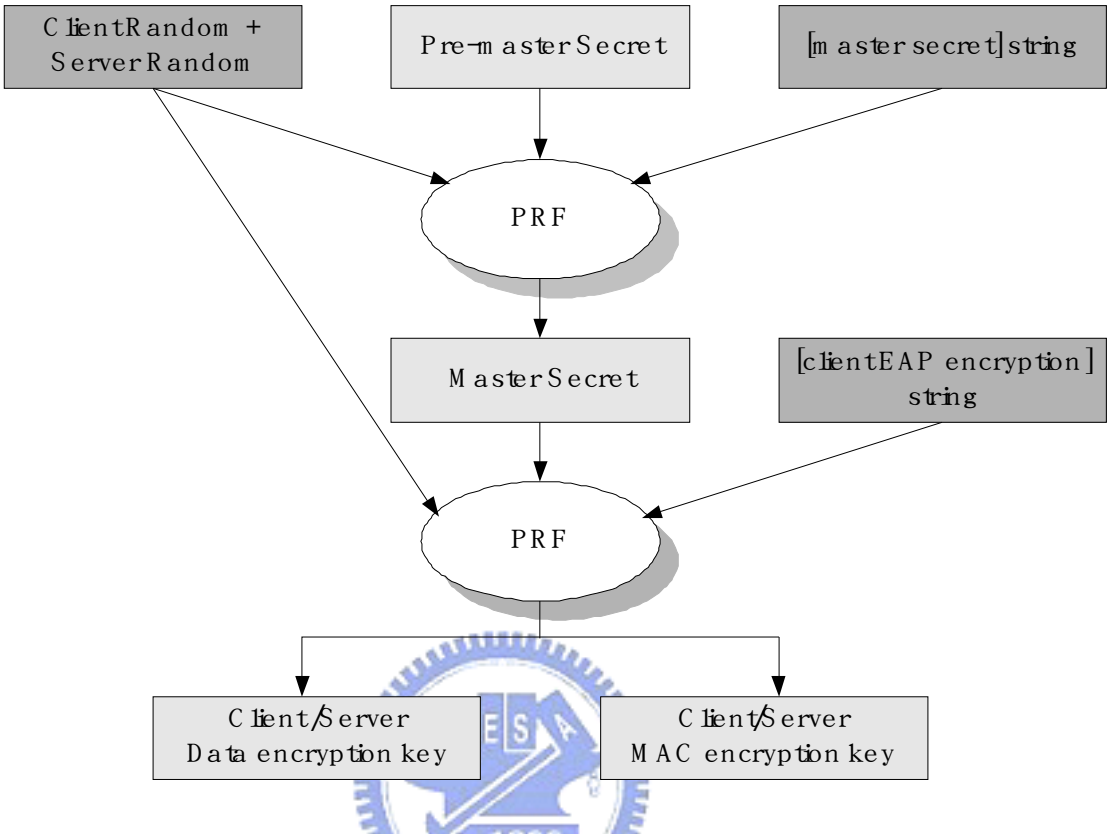

Figure 2-5. The session key derivation of EAP-TLS

2.5 IEEE 802.11i Overview

The IEEE 802.11i is now a draft standard for IEEE 802.11 wireless network security. This upcoming standard 802.11i introduces the Robust Security network (RSN) protocol for establishing a secure communication. The RSN protocol defines several new standards, and also relies on many existing standard such as the current

IEEE 802.1x is included for authentication and key management.

The RSN data privacy protocol is one of main parts of 802.11i for protecting data transfer. It includes many protocols, such as Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) [20]. The basic concepts of security improvement in the data privacy protocol are shown as follows.

1. Encryption key: There is not a single key for every packet in each connection, which makes it harder to break.

2. Packet ordering: The key generation bases on the packet sequence in which it combines secure key and packet sequence. Therefore, the recipient can ignore out of order packets.

3. Identity: The key generation also includes the source and destination MAC addresses. If a hacker intercepts your packets for resending, he or she must pretend to be you unless having another way to re-generate the key.

4. Integrity: Use a secure cryptographic algorithm instead of a simple Cyclic Redundancy Check (CRC).

However, the IEEE 802.11i requires having capabilities that most existing devices don't have, including higher processing power and supports for intensive encryption algorithm. Therefore, we propose a new key management, which is more efficiency and simpler, in my thesis.