

Authentication in Wireless Networks

Prof. Divya Bansal, Sachin Lalar

Sachin509@gmail.com

Punjab Engg. College, Chandigarh

Abstract

Broadband wireless access networks based on WiMAX can provide backhaul support for mobile WiFi hotspots. We consider an integrated WiMAX / WiFi network for different application where the licensed WiMAX spectrum is shared by the WiFi access points to provide Internet connectivity to mobile WiFi users. This type of development is suffering today from different security problems due to the fact that it is a wireless technology. In the cryptographic scenario authentication protocols play an important role. This paper will focus on the importance of this kind of cryptographic tools in the emergent technology of wireless networks. The alternatives for authentication in this setting will be introduced and some of their weaknesses will be pointed out. The Extensible Authentication Protocol (EAP) is widely used in WiFi/802.11 and WiMax/802.16 wireless networks as an authentication solution. This paper uncovers the main threats to EAP and some common EAP methods.

1. Introduction

WiMAX has emerged as a promising technology for broadband access in wireless metropolitan area network (WMAN) environment. One of the potential applications of WiMAX is to provide backhaul support for mobile WiFi hotspots. Traditionally, a WiFi hotspot is connected to the Internet via a wired connection (e.g., digital subscriber line, DSL). However, by using WiMAX-based backbone network to connect WiFi hotspots to the

Internet, costly wired infrastructure can be avoided, and, again, mobile hotspot services can be provided (e.g., for intelligent transportation system [ITS] applications).

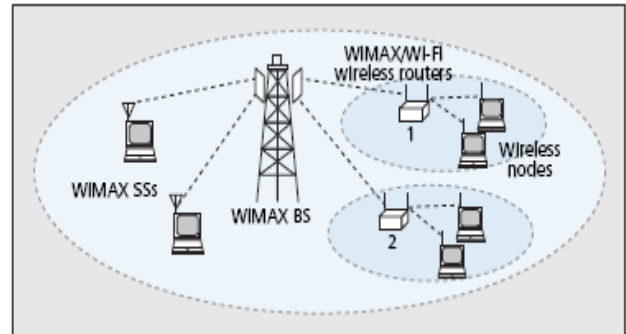


Figure 1: An Integrated Wimax/Wi-Fi network

We consider a system model shown in Fig. 1. In this model a WiMAX base station (BS) operating in a licensed band serves both WiMAX subscriber stations (SSs) and WiFi access points (APs) in its coverage area. The connection between the BS and an SS is dedicated to a single user, while the connection between the AP and the BS is shared among the wireless LAN (WLAN) nodes. Also, the WiMAX BS and WiFi APs are assumed to be operated by different service providers.

Each of the SSs has a fixed bandwidth demand from the BS, while the APs/routers have elastic (i.e., time-varying) demand. For the network model described above, the WiMAX and WiFi service providers have to negotiate with each other to determine the optimal price such that their profits are maximized.[1].

WiMax will provide high-speed network connections and thereby serve as a backbone for IEEE 802.11 wireless LAN hot spots, where

roaming mobile users can access carriers' WiFi services. WiMax could thus offer a less expensive, easier to build infrastructure than the wireline WiFi backbones that DSL, cable, or T1 systems currently provide wireless hotspots based on IEEE 802.11 wireless LAN (WLAN) have become very popular for providing different data services to Internet users [1]. Traditionally, WLAN hotspots are connected to the Internet through a wired network infrastructure (fixed hotspot). However, such a wired infrastructure may not be available in remote rural or suburban areas.

The evolving family of IEEE 802.16 (WiMAX)-based wireless metropolitan area network (WMAN) technologies (i.e., IEEE 802.16a, 802.16d, 802.16e, 802.16g, WiBro) is a promising solution to provide backhaul support for WLAN hotspots. Designed for high-speed broadband wireless access (50–100 Mb/s), IEEE 802.16 supports point-to-multipoint single-hop transmission between a single base station (BS) and multiple subscriber stations as well as multihop mesh networking[2]. In such a network both static and mobile nodes, generally referred to as mesh routers and mesh clients, respectively, communicate *wirelessly* in a multihop fashion.

In an infrastructure wireless mesh network, the mesh routers form a backbone network for the mesh clients to connect to the Internet. Therefore, an integrated 802.16/802.11 network can be used to extend the coverage area of a WLAN and augment the service availability for mobile Internet applications. In such a mobile hotspot, a WLAN access point/router with a dual radio interface connects to a 802.16 base station (BS)/mesh router, and the WLAN traffic is relayed to an Internet gateway through multiple 802.16 base stations operating in mesh mode.

2. Authentication in Wireless Network

Before allowing entities to access a network and its associated resources, the general mechanism is to authenticate the entity (a device and/or user) and then allow authorization based on the identity. The most common access control is binary: It either allows access or denies access based on membership in a group.

Authentication is a security primitive which enables a node to ensure the identity of the peer node it is communicating with. Authentication is the act of establishing or confirming something (or someone) as authentic, that is, that claims made by or about the thing are true. Authenticating an object may mean confirming its provenance, whereas authenticating a person often consists of verifying their identity[4].

The authentication is based on a three-party model: the supplicant, which requires access; the authenticator, which grants access; and the authentication server, which gives permission. The supplicant has an identity and some credentials to prove that it is who it claims to be. The supplicant is connected to the network through an authenticator's port that is access controlled. The authenticator itself does not know whether an entity can be allowed access; that is the function of the authentication server[7].

Layered Framework for Authentication

As shown in Figure 2 the authentication model is a layered one and has well-defined functionalities and protocols defining each layer and the interfaces between them. The access media (Step 1 in Figure 2 can be any of the 802 media: Ethernet, Token Ring, WLAN, or the original media in the serial Point-to-Point Protocol (PPP) link. The EAP specifications provide a framework for exchanging authentication information (Step 2 in Figure 2)after the link layer is established..

It is the function of the transport protocol layer (Step 3 in Figure 2) to specify how EAP messages can be exchanged over LAN, which is what 802.1x (and to some extent some parts of 802.11i) does. The actual authentication process (Step 4 in Figure 2) is the one that defines how and what credentials should be exchanged. Bear in mind that this framework still does not say how the authorization should be done, such as what decisions are made and when. This functionality is completely left to the domain.

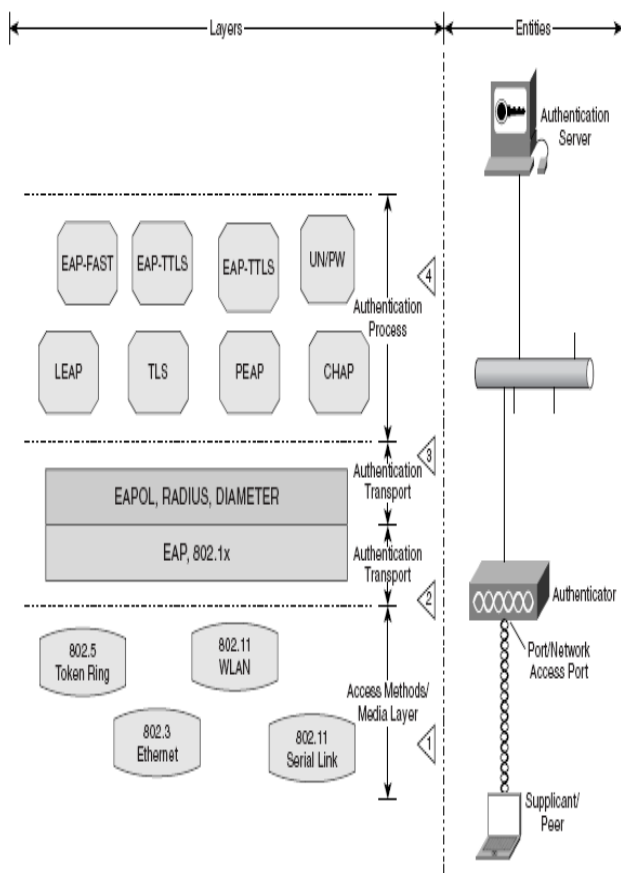


Figure 2: Layered Framework for authentication

3.Extensible Authentication Protocol (EAP)

The Extensible Authentication Protocol (EAP) is an authentication framework that is widely used in WiFi/802.11 and WiMax/ 802.16 wireless networks. EAP is a basis to transfer authentication information between a client and

a network. It provides a basic request/response protocol framework over which to implement a specific authentication algorithm, so called EAP method. Commonly used EAP methods are EAP-MD5, EAP LEAP,EAP-TLS, EAP-TTLS and EAP-PEAP[3].

An EAP infrastructure consists of the following:

- **EAP Supplicant** Computer that is attempting to access a network, also known as an access client.
- **EAP authenticator** An access point or network access server (NAS) that is requiring EAP authentication prior to granting access to a network
- **Authentication server** A server computer that negotiates the use of a specific EAP method with an EAP peer, validates the EAP peer's credentials, and authorizes access to the network. Typically, the authentication server is a Remote Authentication Dial-In User Service (RADIUS) server

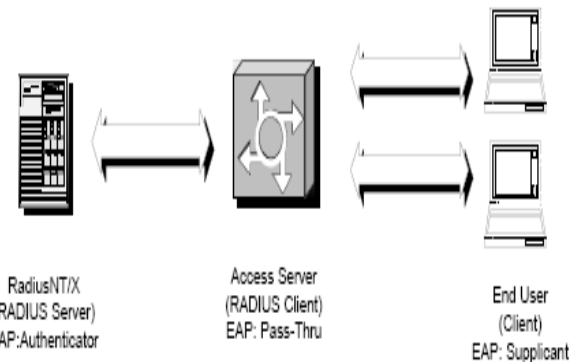


Figure 3 : EAP Authentication

The EAP authentication protocol is based on a challenge-response scheme. Four types of messages are used: REQUEST, RESPONSE, SUCCESS and FAILURE. Firstly, a supplicant sends a connection request to a wireless network through the authenticator. Then a series of REQUEST and RESPONSE messages are exchanged. The length and details of the authentication conversation depend on the

underlying authentication method. The AS uses the SUCCESS or FAILURE message to notify the AP whether the supplicant authentication was successful or not, and the supplicant will be connected to the network as requested in a successful case.

EAP Frames, Messages, and Choreography

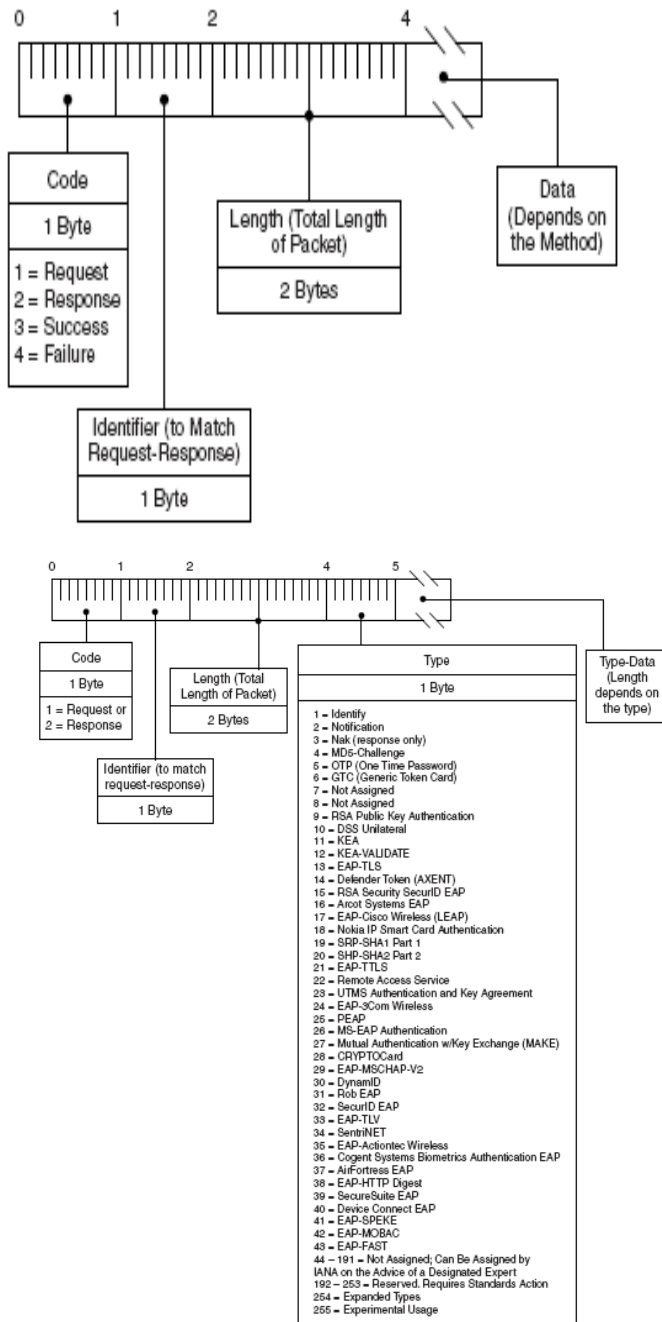


Figure 4: EAP Frame Format

The basic EAP consists of a set of simple constructs: four message types, two message frames, and an extensible choreography. The

four message types are request, response, success, and failure. Figure 4 shows the EAP frame format[4].

The EAP message exchange is basic, as shown in Figure 6. EAP starts after the supplicant has data and link layer connectivity (Step 0 in Figure 5). The communication between the authenticator and the supplicant is done as a request-response paradigm, meaning a message is sent and the sender waits for a response before sending another message[5].

The first exchange (Step 1 in Figure 5) could be an identity exchange. Even though there is an identity message type, the RFC does not guarantee identity semantics and encourages that the authentication mechanisms not depend on this exchange for identity and have their own identity-recognition mechanisms. Moreover, the initial exchange would most likely be in cleartext; therefore, it is a security vulnerability.

In Step 2, all the exchanges between the supplicant, authenticator, and back-end authentication systems are defined by a wide variety of specific RFCs or drafts and authentication mechanisms. Finally, at some point, the authenticator determines whether the authentication is a success or failure and sends an appropriate message to the supplicant (Step 3 in Figure 5).

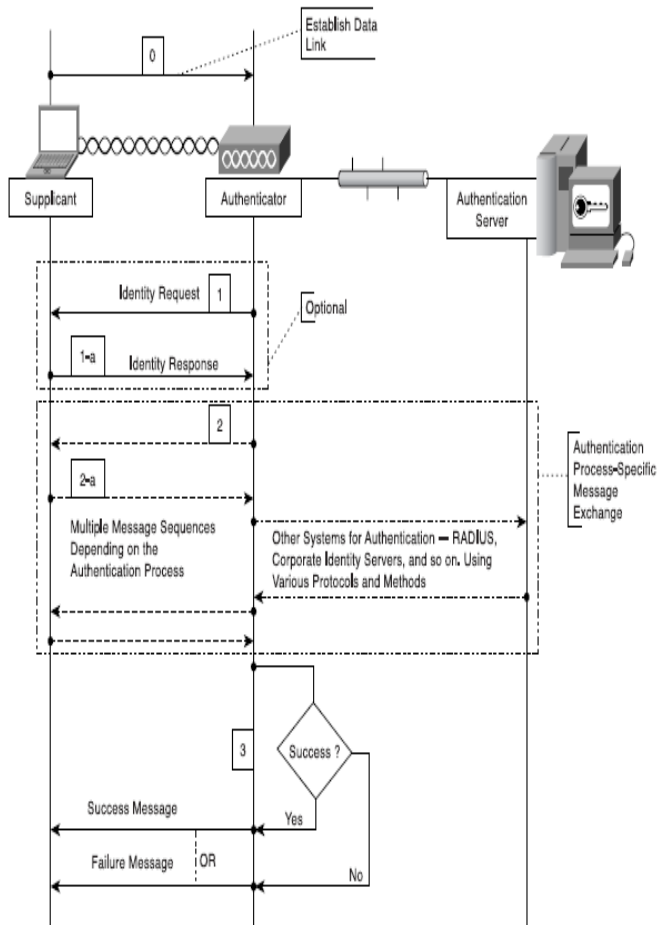


Figure 5: EAP Message Exchange Framework

3.Desired Properties of WLAN Authentication

In this section, five main desired security properties are described, against which threats to EAP methods are analyzed in following sections[3].

➤ Mutual authentication

Mutual authentication is a two-way authentication process between the supplicant and AS. The supplicant ensures that he/she is not communicating with a rogue AS by authenticating the AS. If this property is absent, a rogue AS may be able to mount a Man-In-The-Middle attack to gather private messages from the supplicant. This feature is critical.

➤ Identity privacy

The identity here is referring to supplicant's username instead of the Media Access Control (MAC) address. As discussed in Section 1, EAP authentication conversation starts with the Request-Identity and Response-Identity messages. Since these messages are sent in plaintext, attack can easily discover supplicant's identity by eavesdrop the conversation at the beginning of the process. Thus, EAP methods must take care of hiding supplicant's identity.

➤ Replay attack resistance

If an attacker eavesdrops and records the authentication process of a valid supplicant and replays it to gain the access to the network, a replay attack will occur. Replay attacks may happen even when the attacker does not know the password required for the authentication process. EAP methods must take care to resist this attack.

➤ Dictionary attack resistance

If the supplicant picks up a potentially guessable password and the attacker has access to some data derived from the password in a known algorithm, a dictionary attack may happen. In order to protect against this attack, EAP methods must take care to not reveal such data.

➤ Derivation of strong session keys

One major weakness of using a static session key is that the secret key may eventually be derived from the eavesdropped messages. Any secret is not likely to remain secret forever. Once an attacker discovers the secret key via some attacks, for example dictionary attack, he can decrypt any message that is encrypted with the discovered key. EAP methods that generate dynamic session keys are desired.

4.Security Attacks On EAP

In wireless networks, since EAP authentication data packets are being transmitted via Radio waves rather than over a wire, EAP methods are vulnerable to the following attacks[14]:

- **Impersonation of a user:** an attacker may discover user identities by snooping authentication traffic
- **Impersonation of an authenticator:** an attacker may act as an authenticator and provide incorrect information to supplicants
- **Data alteration:** an attacker may try to modify and spoof EAP packets
- **DoS (Denial of Service):** an attacker may spoof Success/Failure packets or replay EAP packets or generate packets with overlapping identifiers to carry out this attack
- **Dictionary attack:** an attacker may mount an offline dictionary attack by discovering user's password
- **MITM (Man-In-The-Middle):** an attacker can pass through the entire authentication conversation, then hijack the session and act as the user

EAP-MD5 is one of the most popular EAP methods, which provides the base-level EAP support [6]. A one-way hash algorithm is used in combination with a shared secret and a challenge to verify that the supplicant knows the shared secret. There is no mutual authentication and it does not provide a means to derive dynamic Wired Equivalency Privacy (WEP) keys per session. Although it is not easy to gain an EAP-MD5 packet, a captured one is easy to crack. If the attacker can obtain the challenge and the hashed response, they can then run a program off-line with the same algorithm as the supplicant, plugging in words from a dictionary until their hashed response matches the supplicant's. They then know the supplicant's password and can steal its identity, which is passed in clear text, to gain access to the network. This process is made much easier in wireless LANs where the challenge and response are passed through the air. As a result, this method is open to a dictionary attack[7].

With just client side authentication, EAP-MD5 is also vulnerable to Man-In-The-Middle attacks. It can allow a client to talk to a rogue AP, which gives the malicious person access to all of the data passed to and from the end user. In addition, a malicious person can even hijack a supplicant's session. The malicious person could pretend to be a valid AP; the user connects to the rogue AP; the rogue AP pretends to be the valid supplicant and passes all the supplicant's responses as its own. The missing of mutual authentication is a major flaw in EAP-MD5[6].

LEAP is developed by Cisco system for use on WLANs that use Cisco 802.11 wireless devices. It uses a log-on password as a shared secret. LEAP offers mutual authentication instead of a one-way authentication between supplicant and AS. This feature eliminates the MITM attacks by rogue APs. It encrypts data transmissions using dynamically generated WEP keys.[10] With LEAP, session keys are unique to users and not shared among them. However, LEAP is vulnerable to dictionary attacks [8]. In March 2003, Joshua Wright disclosed that LEAP was vulnerable to dictionary attacks. A short time later Wright released ASLEAP, a tool to automate attacks over LEAP.[9] This is because LEAP mainly relies on MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2) to protect supplicant's credentials. MS-CHAPv2 sends usernames in clear text and does not use a SALT in its hashes so that dictionary and brute force attacks can be mounted[9]. In practical, more cracking tools to LEAP have already been created, such as THC LEAP and ANWRAP LEAP. CISCO released EAP-FAST as a replacement for LEAP after one year of Wright's disclosure.

EAP-TLS is completely password cracking resistant because it does not rely on user passwords [13]. EAP-TLS provides mutual authentication between the supplicant and AS based on X.509 certificates. It eliminates MITM attacks and rogue APs can be detected. It also

dynamically generates and distributes user-based and session-based encryption keys to secure connections. Therefore, supplicant's identity and password are not revealed. One drawback of EAP-TLS is that it requires both the supplicant and AS to have valid certificates. This brings significant management complexity. The AP creates a RADIUS Access Request using the supplicant's identity and sends it to the AS. The AS then provides its certificate to the supplicant and asks for the supplicant's certificate. The supplicant provides its certificate to AS if the received AS's certificate is valid. After the AS validates the supplicant's certificate. EAP-TTLS and EAP-PEAP are tunneled methods. EAP-TTLS and EAP-PEAP provide better security, since EAP-TTLS and EAP-PEAP take the benefits from EAP-TLS and add additional features[11].

5. Conclusion

EAP-MD5 and EAP-LEAP are found not sufficiently secure because of their vulnerability to dictionary attacks. EAP-TLS provides strong security, while EAP-TTLS and EAP-PEAP provide better security, since EAP-TTLS and EAP-PEAP take the benefits from EAP-TLS and add additional features. Dictionary attack is the most common and high risk threat to some EAP methods. This vulnerability can be reduced by using strong password policy. Good passwords should never contain recognizable words and their length should be greater than or equal to eight and contain a mix of numbers, letters and special characters. However, we should note that no single security solution is likely to address all security risks. In industry, good authentication methods, for example EAP-TLS, usually have difficulties with deployment and management.

References

1. Dusit Niyato and Ekram Hossain, TRILabs and University of Manitoba, "Integration of WiMAX and WiFi".
2. Dusit Niyato and Ekram Hossain, TRILabs

- and University of Manitoba," Integration of IEEE 802.11 WLANs with IEEE 802.16-Based Multihop Infrastructure.
3. Jyh-Cheng Chen and Yu-Ping Wang "Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience", 2005.
4. Philip kwan, "801.1x Authentication & Extensible Authentication protocol(EAP)", May, 2003
5. B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowitz. Extensible authentication protocol (EAP). The Internet Engineering Task Force -Request for Comments: 3748, June 2004.
6. George C. Ou, "Enterprise Level Wireless LAN Security", 2002:A Study of the MD5 Attacks: Insights and Improvements
7. Tunnels in Hash Functions: MD5 Collisions Within a Minute Vlastimil Klima Prague, Czech Republic J. Black _ M. Cochran _ T. Highland March 3, 2006
8. Dictionary Attack on Cisco LEAP. Tech Note, available at <http://www.cisco.com/warp/public/707/cisco-sn-20030802-leap.shtml>.
9. George C. Ou, "LEAP: A looming disaster in Enterprise Wireless LANs", 2004
10. Cisco Security Notice: Dictionary Attack on Cisco LEAP Vulnerability, 2004.
11. Palekar, A., et al., "Protected EAP Protocol (PEAP)", Work in Progress, July 2004
12. Jim Burns, "Selecting an Appropriate EAP Method for Your Wireless LAN", 2003. Aboba, B. and D. Simon, "PPP EAP TLS Authentication Protocol", RFC 2716, October 1999.
13. Funk, P. and S. Blake-Wilson, "EAP Tunneled TLS Authentication Protocol (EAPTTLS)", August 2004.
14. Identifying and responding to wireless attacks: Chris Hurley 802.11 Wireless Attacks: Pavol Lupták