A Threat Analysis of The Extensible Authentication Protocol

Lei Han

Student #: 100304821

April, 2006

Supervised by Professor Michel Barbeau

School of Computer Science

Carleton University

Honors Project Report

Acknowledgement

I wish to express my sincere gratitude to Professor Michel Barbeau, my supervisor, for his encouragement and guidance during the course of this project. Thank you for always being there and helping me whenever I needed.

Abstract

Security is always a major concern for wireless LAN development. This type of development is suffering today from different security problems due to the fact that it is a wireless technology. Extensible Authentication Protocol (EAP) is widely used in WiFi/802.11 and WiMax/802.16 wireless networks as an authentication solution. This report uncovers the main threats to EAP and some common EAP methods. Specifically EAP-MD5, EAP-LEAP, EAP-TLS, EAP-TTLS and EAP-PEAP are reviewed in detail. A threat analysis is presented and the threat is ranked from three aspects: likelihood, impact, and risk.

Table of Contents

Section Title **Page**

Table of Figures

Figure **Page**

Table of Tables

Table **Page**

1. Introduction

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. Within the EAP framework, three entities are involved in the authentication process (Fig. 1): Supplicant, Authenticator, and Authentication Server [1]. The supplicant is a user that is trying to access the network. It is also known as the peer. The authenticator is an access point (AP) that is requiring EAP authentication prior to granting access to a network. It provides users a point of entry into the network. The authentication server (AS) is the entity that negotiates the use of a specific EAP method with an EAP supplicant, then validates the supplicant, and authorizes access to the network. Typically, the supplicant is a mobile station (MS) and the authentication server is a Remote Authentication Dial-In User Service (RADIUS) server.

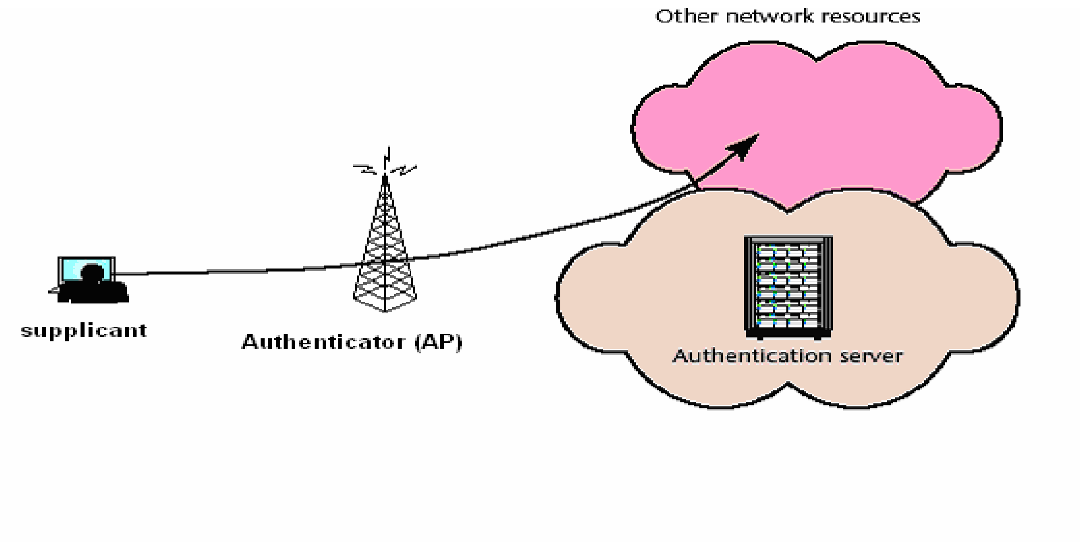

Figure 1: Entities in EAP Framework

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. The general message flow is shown in Figure 2. The AP is unaware of any details of the authentication process. It only cares about the AS's final decision, and forwards packets back and forth between the supplicant and the AS. At the same time, the AP listens for the SUCCESS or FAILURE message from the AS and ends the authentication conversation by passing by the SUCCESS/FAILURE message to the supplicant.

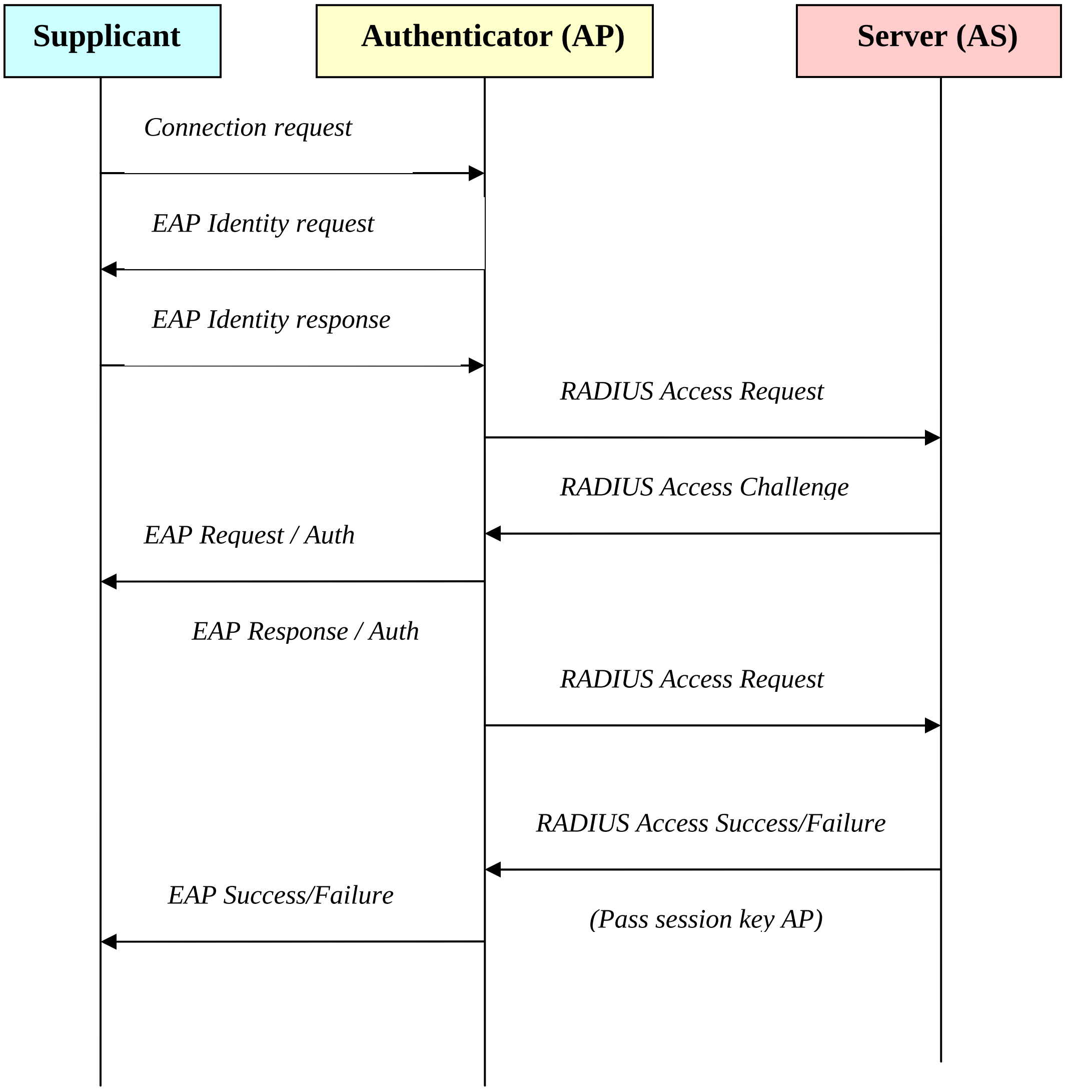

Figure 2: EAP Message Flow

EAP runs over data link layers without requiring an Internet Protocol (IP) and it provides its own support for duplicate elimination and re-transmission. The EAP mechanism makes the authentication process flexible by using a backend authentication server, which may implement some or all authentication methods. EAP methods can be extended by plugging-in at both the supplicant and authentication server ends of a connection. This capability provides the flexibility to allow for several authentication methods.

Although EAP provides authentication flexibility through the use of EAP types, the entire EAP conversation might be sent as clear text. This is problematic in WLAN, in which the attacker can be located outside of your business. EAP is widely used today and attacks have been found from industry. Possible attacks are denial of service (DoS), dictionary attack, man-in-the-middle attack, impersonation of authenticator, impersonation of user, and weaken authentication method. [1]

This project is focus on commonly used EAP authentication methods: EAP-MD5, EAP-LEAP, EAP-TLS, EAP-TTLS, and EAP-PEAP. Security flaws in each method are uncovered and an analysis of the security threats to each method is presented using a methodology described in Ref. [8]. A complete summary table (Table 6) of these five EAP methods can be found in the Appendix.

Desired properties of WLAN authentication is described in Section 2. The methodology used to analyze threats to EAP methods are presented in Section 3. Section 4 contains the description and analysis of main threats to EAP and EAP methods. The conclusion can be found in Section 5.

2. 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. A complete summary table (Table 5) can be found in the Appendix.

- **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.

3. Threat Analysis Methodology

In this project, the methodology described in Ref. [8] is used to analyze threats to EAP methods. The analysis is conducted from three aspects: Likelihood, Impact, and Risk; such that we can have a clear view on the cost/effort and benefit/damage of a specific threat. The “occurrence Likelihood” and “Impact” are estimated with values from 1 to 3. The larger the number is, the more likely a threat could happen and more critical its impact is. Risk is a measurement for overall critical degree of a threat. Its value can be calculated by multiplying the corresponding “occurrence Likelihood” value and **“**Impact” value. Therefore the possible values for Risk are 1 to 4, 6 and 9. As shown in Table1, the possible values of Likelihood are Unlikely, Possible and Likely. A threat is Unlikely to occur if it is very difficult for an attacker to solve technical problems and the motivation is very low. If an attacker could solve technical difficulties without too much effort and the threat will bring attractive motivation, then the threat is possible to occur. The Likelihood is Likely if there is a high motivation and no technical difficulties for an attacker to mount a threat. This could happen if the system has flaws to protect against the threat. The main factors of Likelihood are motivation and technical difficulty. If the motivation is very high, it could even drive people to solve technical difficulties. The Impact evaluates a threat’s consequences. It has two aspects: user and system. The Impact is Low if involved parties are not harmed very strongly and the damage is repairable. For example, only a limited number of users are annoyed or the system is down for a very short period. The Impact is Medium when the damage is limited in terms of money, duration and scope from either user or system perspective. Very serious damages make the Impact to be High. A serious damage could be a big financial loss or a long time system outage. The Risk is an indicator that tells people what should be done to a threat. The Likelihood and Impact value to a threat should be ranked independently. These two values affect the Risk value but not each other.

Table 1: Methodology Summary

Risk		Likelihood *	Impact	Action
Value	Rank	Value(Rank)	Value(Rank)	
Minor	1	Unlikely (1)	Low (1)	no primary need for counter measures
	2	Unlikely (1)	Medium (2)	
		Possible (2)	Low (1)	
	3	Unlikely (1)	High (3)	
		Likely (3)	Low (1)	
Major	4	Possible (2)	Medium (2)	should be fixed as soon as possible
Critical	6	Possible (2)	High (3)	should be addressed with high priority
		Likely (3)	Medium (2)	
	9	Likely (3)	High (3)	

The analysis with this methodology is subjective. There are limitations due to the author's knowledge. The values ranked in later sections are based on information gathered during this project. Therefore, the result might be different compare to other people's work.

4. Security attacks to EAP and EAP methods

Wireless networks are inherently vulnerable to several network attacks due to the broadcast nature of the wireless radio signals. Malicious users are able to passively eavesdrop on the EAP packets and could potentially access information from the packets. It is also possible to actively transmit EAP packets that can attack the network. In this section, an overview of security attacks to EAP is given. EAP methods are developed to mitigate those attacks but each single method has its own flaws based on the properties it has. Main threats to EAP methods can be grouped into three categories: Secret-key methods, Public-key methods, and Tunneled methods. (Refer to Table 5 in Appendix for a summary of desired properties of EAP methods.)

4.1 Overview of security attacks to 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 [1]:

- **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 my 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

4.2 Main attacks to EAP methods

4.2.1 Secret-Key Approach

In secret-key authentication methods, also known as shared-key or symmetric-key methods, the supplicants and AS establish trust by proving to each other the knowledge of a shared secret key.

The advantage of secret-key authentication methods is that they require little computational power, which is an important feature to many wireless devices, for example, mobile VoIP phones. Since most supplicants choose bad passwords, in which they are used to derive the shared secret, it is easy for an attacker to extract the secret key from captured encrypted messages using dictionary attacks. Although there are some EAP authentication methods, for example EAP-SRP that do protect supplicant's password from dictionary attack, these methods require much more power than other secret-key methods. It is also difficult to securely distribute the shared secret to both parties. EAP-MD5 and EAP-LEAP, two secret-key authentication methods, are discussed here after.

4.2.1.1 EAP-MD5

EAP-MD5 is one of the most popular EAP methods, which provides the base-level EAP support [14]. 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 [12], which is *likely* to happen with a *high* impact.

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 rogue AP can take control of the connection if it is a successful authentication and it can send a FAILURE message to fool the supplicant. The missing of mutual authentication is a major flaw in EAP-MD5. There are no critical technical difficulties for an attacker to solve in order to mount the attacks discussed above. This flaw makes AP impersonation and MITM attacks with a *high* impact *likely* to occur. The user impersonation and data alteration is *unlikely* to occur since there is no attractive motivation to do so. Since a limited number of users may be affected by user impersonation, the impact is considered to be *low*. Depends on the data “Data Alteration” attack altered, the impact could be *medium*. Refer to Table 2 for the ranking.

From the above descriptions of these weaknesses, EAP-MD5 is typically not suitable for wireless LAN implementations, especially when strong security is required [12].

4.2.1.2 EAP-LEAP (Lightweight Extensible Authentication Protocol)

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. With LEAP, session keys are unique to users and not shared among them. However, LEAP is vulnerable to dictionary attacks [2]. 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. Although, theoretically LEAP is secure if complex enough passwords are used [15]. By complex enough, we mean it is computationally infeasible to attempt an offline dictionary or brute force attack. Only few organizations have such password enforcement policies. Moreover, even an organization with such a policy, people may write down the complex passwords to remember them. In practical, some cracking tools to LEAP have already been created, such as ASLEAP, THC LEAP and ANWRAP LEAP [11]. An attacker now can crack the majority of enterprise WLAN that running LEAP in a few minutes without any detection since the attack is passive and offline. Since most LEAP implementations have the single sign-on capabilities of most RADIUS servers, the usernames and passwords cracked are usually the same for some common user databases, such as Windows Domain Authentication. This case is even worse than having no encryption at all on the WLAN because an attacker could not only gain access to the WLAN, but also gain the supplicant's credentials to access critical data directly. Therefore, the author believes that the dictionary attack to LEAP is *likely* to occur, the impact is *high*, and the risk is *critical*. Considering this risk, Cisco recommends users move to other EAP methods, such as EAP-FAST, EAP-TLS or EAP-PEAP, to mitigate the dictionary attack [13]. Since mutual authentication is provided in this method, the MITM and AP impersonation attacks are *unlikely* to happen, the impact is *high*, but the risk is *minor*. Other attacks, i.e. user impersonation, data alteration and DoS are not found in any paper during this project, so the likelihood is considered to be *unlikely*. Their impacts follow the same discussion of EAP-MD5. Refer to Table 2 for ranking.

Table 2: Risk Evaluation of Secret-Key Approach

Threat	EAP-MD5			EAP-LEAP		
	Likelihood	Impact	Risk	Likelihood	Impact	Risk
User Impersonation	1	1	1	1	1	1
AP impersonation	3	3	9	1	3	3
Data alteration	1	2	2	1	2	2
DoS	2	2	4	1	2	2
Dictionary Attack	3	3	9	3	3	9
MITM	3	3	9	1	3	3

4.2.2 Public-Key Approach

Unlike the secret-key approach, the public-key methods use a public and private key pair. A message is encrypted with the public key can only be decrypted with the corresponding private key. To insure that a supplicant's public key is valid and to prevent impersonation, the AS and supplicant need to establish trust through a Certification Authority (CA). A CA is an independent third party that issues certificates. EAP-TLS is a public-key method.

4.2.2.1 EAP-TLS (Transport Layer Security)

EAP-TLS is completely password cracking resistant because it does not rely on user passwords [3]. 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.

Figure 3 shows the brief message flow of EAP-TLS in a WLAN network. 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, it will send the result message *RADIUS Access Success/Failure* to deny or permit access to the network.

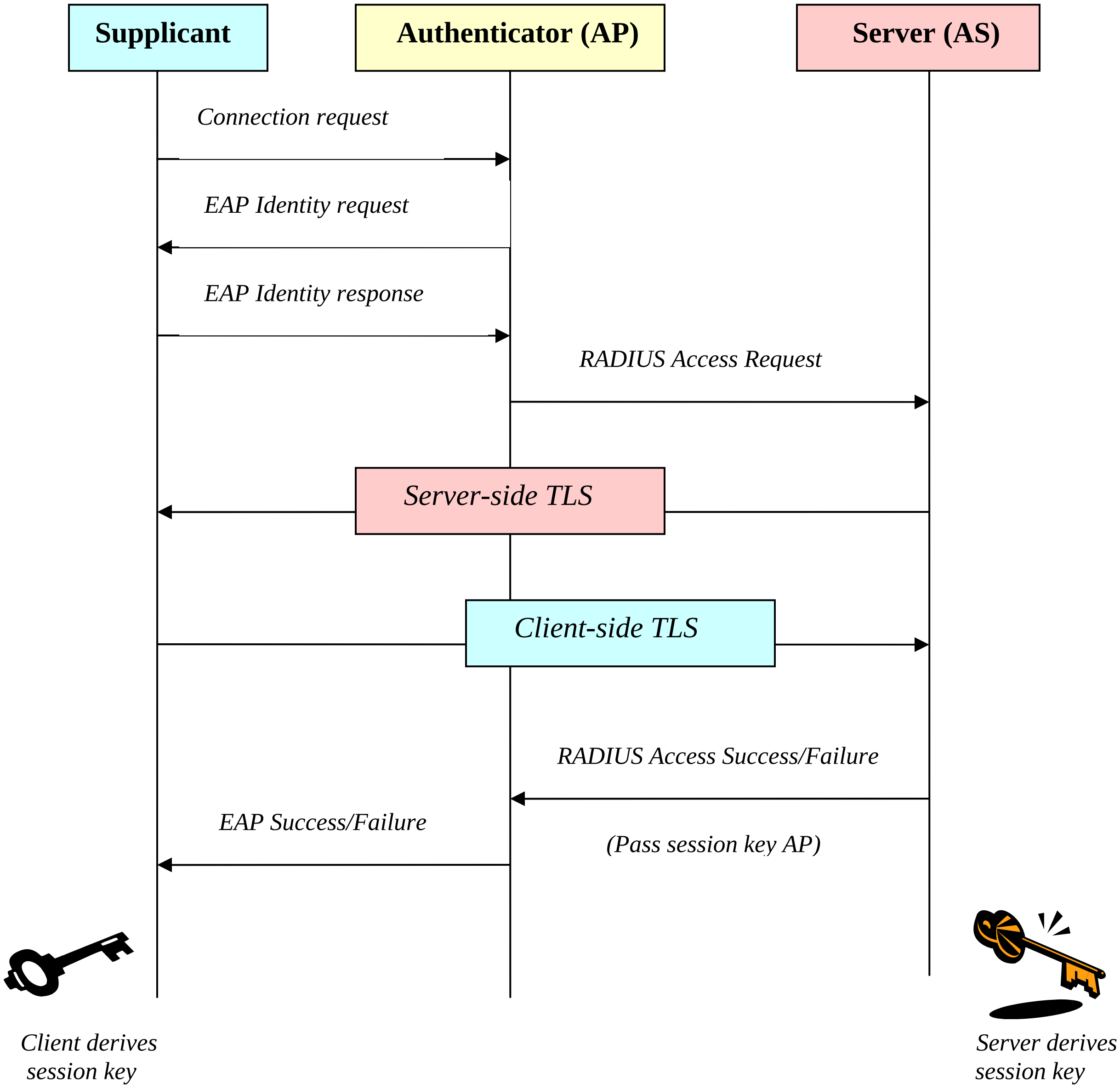

Figure 3: EAP-TLS Message Flow [10]

As discussed, EAP-TLS is considered to be very secure [12]. It is widely used and well tested. EAP-TLS resists most attacks, such as replay and MITM attacks. Therefore all attacks discussed in Section 4.1 are considered *unlikely* to occur. Their impacts follow the same discussion in Section 4.2.1.1. Refer to the summary table (Table 3) for ranking.

Table 3: Risk Evaluation of Public-Key Approach

Threat	**EAP-TLS**		
	Likelihood	Impact	Risk
User Impersonation	1	1	1
AP impersonation	1	3	3
Data alteration	1	2	2
DoS	1	2	2
Dictionary Attack	1	3	3
MITM	1	3	3

4.2.3 Tunneled Approach

EAP-TTLS and EAP-PEAP are tunneled methods. The main benefit of a tunnel is that it provides identity privacy. Using tunnels, the tunnel methods can hide the supplicant's identity from eavesdropping by hiding the EAP Response Identity message in the secure tunnel. Since the AS does not authenticate the supplicant in the first phase, the supplicant can send the username through the secure tunnel established after the TLS handshake to initiate the second phase. Moreover, EAP-TTLS and EAP-PEAP can provide mutual authentication that is as secure as EAP-TLS even when only legacy client-authentication methods are available. Since the secure tunnel established in the first phase hides the messages sent in the second phase, the supplicant and AS can be sure that the client authentication is as secure as EAP-TLS. Since attackers sniffing the tunneled session must break the secure EAP-TLS tunnel to mount attacks, such as replay attack or dictionary attack, EAP-TTLS and EAP-PEAP are considered to be very secure [12]. Even when the authentication method is vulnerable to those attacks, it is no longer vulnerable to them in the tunneled second phase. However, there are studies that found a

MITM attack in these tunneled protocols [6]. The tunneled protocols require the session key from the first phase, which is used to encrypt the tunnel, to be the session key for the message protection. They sometimes allow supplicant to skip the tunneling and to proceed directly to the second phase. A MITM attack may happen if an attacker can hijack a valid supplicant's session. Fortunately, people are taking care of these problems and have proposed possible solutions [7]. Thus, EAP-TTLS and EAP-PEAP are still very secure if these proposed solutions are applied. Therefore, all attacks discussed in Section 4.1 are considered *unlikely* to occur. There impacts follow the same discussion in Section 4.2.1.1. Refer to the summary table (Table 4) for ranking.

4.2.3.1 EAP-TTLS (Tunneled Transport Layer Security)

EAP-TTLS is an extension of EAP-TLS [5]. Its authentication process has two phases: the TLS handshake phase and TLS tunnel phase. During the first phase, the AS is authenticated to the supplicant using an X.509 certificate. However, unlike EAP-TLS, EAP-TTLS only requires server-side certificates. A secure TLS tunnel is established after the TLS handshake. In phase two, other information, such as accounting information is exchanged through the secure TLS tunnel. EAP-TTLS also supports identity hiding where the AP is only aware of the anonymous username used to establish the TLS channel during the first phase, but not the individual supplicant authenticated during the second phase. EAP-TTLS allows the use of legacy password-based protocols with existing authentication databases, while protecting the security of these legacy protocols against eavesdropping and MITM attacks.

4.2.3.2 EAP-PEAP (Protected EAP)

EAP-PEAP provides wrapping of the EAP methods within TLS [4]. Thus, the EAP messages encapsulated inside the TLS tunnel are protected against various attacks. The basic principal of EAP-PEAP and EAP-TTLS are identical. Unlike EAP-TTLS, however, EAP-PEAP can only use EAP methods in phase two, while EAP-TTLS can use either EAP or non-EAP methods.

Table 4: Risk Evaluation of Tunneled Approach

Threat	**EAP-TTLS**			**EAP-PEAP**		
	Likelihood	Impact	Risk	Likelihood	Impact	Risk
User Impersonation	1	1	1	1	1	1
AP impersonation	1	3	3	1	3	3
Data alteration	1	2	2	1	2	2
DoS	1	2	2	1	2	2
Dictionary Attack	1	3	3	1	3	3
MITM	1	3	3	1	3	3

5. Conclusion

In this report, five desired properties of WLAN authentication protocols were presented. Five most commonly used EAP methods: EAP-MD5, EAP-LEAP, EAP-TLS, EAP-TTLS, and EAP-PEAP are discussed. 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. Also passwords should periodically expire.

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. Refer to Table 6 for deployment comparison among EAP methods.

6. Appendix

Table 5: Summary of Desired Properties of EAP Methods

	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	PEAP
Mutual authentication	No	Yes	Yes	Yes	Yes
Identity privacy	No	No	No	Yes	Yes
Replay attack resistance	No	Yes	Yes	Yes	Yes
Dictionary attack resistance	No	No	Yes	Yes	Yes
Derivation of strong session keys	No	Yes	Yes	Yes	Yes

Table 6: Summary of EAP Authentication Method

	EAP-MD5	EAP-LEAP	EAP-TLS	EAP-TTLS	PEAP
Server Authentication	None	Password hash	Public key (certificate)	Public key (certificate)	Public key (certificate)
Supplicant Authentication	Password hash	Password hash	Public key (certificate)	MS-CHAP(v2), EAP, CHAP	EAP
Dynamic Key Generation	No	Yes	Yes	Yes	Yes
Ease of Deployment	Easy	Hard	Hard	Moderate	Moderate
Over all Security Performance	Poor	Ok	Good	Good	Good
Software support	Multiple OS Support	Multiple OS Support	Win200 and XP	Multiple OS Support. Requires Cisco 802.11 Wireless Card	Native to Win XP

7. References

[1] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz. Extensible authentication protocol (EAP). The Internet Engineering Task Force -Request for Comments: 3748, June 2004.

[2] Dictionary Attack on Cisco LEAP. Tech Note, available at http://www.cisco.com/ warp/public/707/cisco-sn-20030802-leap.shtml.

[3] Aboba, B. and D. Simon, "PPP EAP TLS Authentication Protocol", RFC 2716, October 1999.

[4] Palekar, A., et al., "Protected EAP Protocol (PEAP)", Work in Progress, July 2004.

[5] Funk, P. and S. Blake-Wilson, "EAP Tunneled TLS Authentication Protocol (EAP-TTLS)", Work in Progress, August 2004.

[6] N. Asokan, Valtteri Niemi, and Kaisa Nyberg. Man-in-the-Middle in Tunnelled Authentication Protocols. Cryptology ePrint Archive, Report 2002/163, 2002.

[7] Jose Puthenkulam, Victor Lortz, Ashwin Palekar, and Dan Simon. The Compound Authentication Binding Problem. IETF Internet Draft, draft-puthenkulam-eap-binding-04.txt, October 2003.

[8] ETSI. Telecommunications and internet protocol harmonization over networks (TIPHON) release 4; protocol framework definition; methods and protocols for security; part 1: Threat analysis. Technical Specification ETSI TS 102 165-1 V4.1.1, 2003.

[9] M. Barbeau, *WiMax/802.16 Threat Analysis*, 1st ACM Workshop on QoS and Security for Wireless and Mobile Networks (Q2SWinet), Montreal, 2005, pp. 8-15.

[10] Jyh-Cheng Chen and Yu-Ping Wang "Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience", 2005.

[11] The Unofficial 802.11 Security Web Page: http://www.drizzle.com/~aboba/IEEE/

[12] Jim Burns, "Selecting an Appropriate EAP Method for Your Wireless LAN", 2003.

[13] Cisco Security Notice: Dictionary Attack on Cisco LEAP Vulnerability, 2004.

[14] George C. Ou, "Enterprise Level Wireless LAN Security", 2002.

[15] George C. Ou, "LEAP: A looming disaster in Enterprise Wireless LANs", 2004.

8. Abbreviations

AP	Access Point
AS	Authentication Server
CA	Certificate Authorities
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EAP-FAST	EAP-Flexible Authentication via Secure Tunneling
EAP-LEAP	EAP-Light Extensible Authentication Protocol
EAP-MD5	EAP-Message Digest 5
EAP-PEAP	EAP-Protected EAP
EAP-TLS	EAP-Transport Layer Security
EAP-TTLS	EAP-Tunnel Transport Layer Security
LAN	Local Area Network
MAC	Media Access Control
MINM	Man-In-The-Middle
MS	Mobile Station
MS-CHAPv2	Microsoft Challenge Handshake Authentication Protocol version 2
IP	Internet Protocol
RADIUS	Remote Authentication Dial-In User Service
TLS	Transport Layer Security
VoIP	Voice over Internet Protocol
WEP	Wired Equivalent Privacy

WLAN	Wireless Local Area Network