ISSN:0975-9646

A Dynamic Extensible Authentication Protocol for Device Authentication in Transport Layer

Raghavendra.K[1] , G. Raghu[2] , Sumith N[2]

[1]*Dept of CSE, P.A.College of Engineering*
[2]*Dept of CSE, Srnivas institute of technology*

Abstract-- Wireless local area networks (wireless LANs, or WLANs) are changing the landscape of computer networking. Wireless communications are inherently more open to attack than wired data transfer, as its physical layer is not contained in the wire. Extensible Authentication Protocol –Transport Layer Security is completely password cracking resistant because it does not rely on user passwords. Extensible Authentication Protocol –Transport Layer Security provides mutual authentication between the supplicant and authentication server based on X.509 certificates. It eliminates MITM attacks and rogue access point's can be detected.

This paper addresses the security problem by proposing a system which involves Client identity protection method that when implemented prevents unauthorized user access and thus protecting or encrypting the data against malicious manipulation. Proposed system provides mutual authentication between the supplicant (User) and Authentication server based on X.509 certificates.

Keywords-EAP, MITM

I. Introduction

Wireless networks offer the benefits of increased productivity, easier network expansion, flexibility, and lower the cost of ownership. In addition Wireless LAN Systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Following the increasing demand for wireless data access, different kind of wireless communication technologies are being developed continually.[8]

On the other hand, security considerations continue to be a major challenge in the wireless network set-ups. Lack of security and inflexible authentication is often cited as a major barrier to the growth of e-commerce (electronic commerce) into m-commerce (mobile commerce). Wireless LANs, unlike the relative simplicity of wired Ethernet deployments, broadcast radio-frequency (RF) data for the Client stations to hear. This presents new and complex security issues requiring additional policies to be incorporated in every WLAN deployment.

Wireless LANs require strict User authentication, Data privacy and Data Integrity to prevent unauthorized access to network resources and protect data from modification or destruction.

This paper addresses the security problem by proposing a system which involves Client identity protection method that when implemented prevents unauthorized user access and thus protecting or encrypting the data against malicious manipulation. Proposed system provides mutual authentication between the supplicant (User) and Authentication server based on X.509 certificates. It eliminates MITM attacks and from rogue AP's. Provides better secure authentication this project can be used in telecommunication applications, for wi -fi authentication, it has wide scope for different applications.

II. How EAP works

The Point-to-Point (PPP) Extensible Authentication Protocol (EAP) (RFC 2284) is an authentication protocol defined by the Internet Engineering Task Force (IETF) that typically rides on top of other protocols such as 802.1x, RADIUS, PPP. Through the use of EAP, support for a number of authentication schemes may be added, including smart cards, Kerberos, Public Key (PKI), One Time Passwords (OTP), and others.[1]

EAP creates a standard message structure to authenticate the Client to the network. Depending on the authentication protocol agreed upon by the Client and the server, the details in the message exchange may vary. Figure 2.1 shows us the general message flow that occurs between the EAP Client, Authenticator and Authentication server. The steps involved in the EAP conversation are:[4]

1. The EAP Client connects to the network and tries to access information on the network.
2. The Authenticator responds to the Client by asking for its identity.
3. The Client responds to the Authenticator with its identity information.
4. The Authenticator forwards the Client's identity information to the Authentication Server using the necessary protocol agreed upon by the Authentication Server and the Authenticator or Client.
5. The Authentication Server responds with a challenge to the Authenticator and specifies the EAP authentication type supported by the Authentication server. This message is transmitted over the RADIUS protocol back to the Authenticator.
6. The Authenticator forwards the challenge back to the Client with the authentication type requested by the Authentication Server.
7. The Client examines the challenge and determines if it can support the requested EAP authentication protocol. If it cannot support the authentication type requested by the Authentication Server, the Client will issue a NAK request and try to negotiate an alternative authentication method. If the Client can support the authentication type

requested by the Authentication Server, it responds with its credential information.

8. The Authenticator relays the Client's credentials to the Authentication Server using the RADIUS protocol.

9. If the Client's credentials are valid, the Authentication Server authenticates and authorizes the Client. Otherwise, the Client is rejected and the appropriate RADIUS Access-Accept or Access-Reject message is sent back to the Authenticator using the RADIUS protocol.

10. The Authenticator receives the RADIUS Access-Accept or Access-Reject message and configures the network access accordingly.

11. Upon receiving the RADIUS ACCEPT packet, the Authenticator transitions the Client's port to an authorized state and the network traffic is forwarded.

III .Remote Authentication Dial-in User Service

A. Overview

The Remote Authentication Dial-in User Service (RADIUS) (RFC 2865) is an IETF-defined Client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service [3]

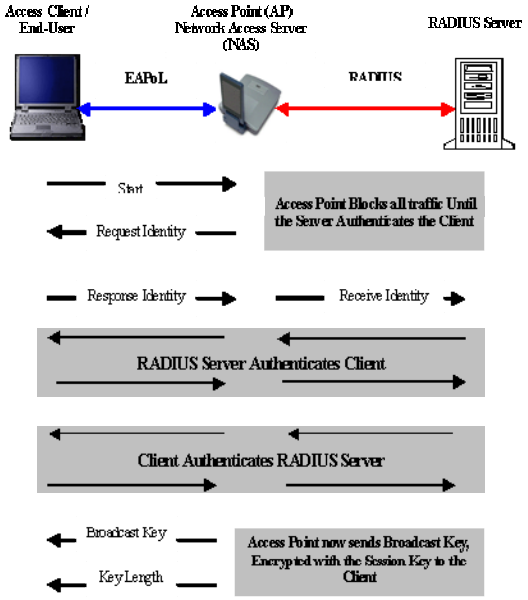

Fig2.1: IEEE 802.1x and EAP Message Exchange

[RFC2865]. It is commonly used to provide centralized Authentication, Authorization, and Accounting (AAA) for dial-up, virtual private network, and, wireless network access.

The software for a RADIUS server includes three parts: an Authentication server, Client protocols and an Accounting server. These pieces can all run on one machine or on separate ones outfitted with different operating systems. Broadly speaking it works by having a user dial in to a remote access server and pass logon name and password information to it. The information is forwarded to a RADIUS Authentication Server that validates the user and returns the information necessary for the access server to initiate a session with the user. The user repeats this process to initiate every session. A dictionary file kept in the RADIUS database determines the types of attributes that can be included in the user profile. The user profile is a file containing authentication security and configuration information for each user.

B. Extensible Authentication Protocol (EAP) over RADIUS

EAP over RADIUS is a transport mechanism for passing EAP messages of any EAP type by the RADIUS Client (access point) to a RADIUS server for authentication. EAP is supported in the RADIUS and allows for new authentication types to be used over links running on the PPP protocol. To support EAP, RADIUS includes two new attributes - EAP-Message and Message-Authenticator.

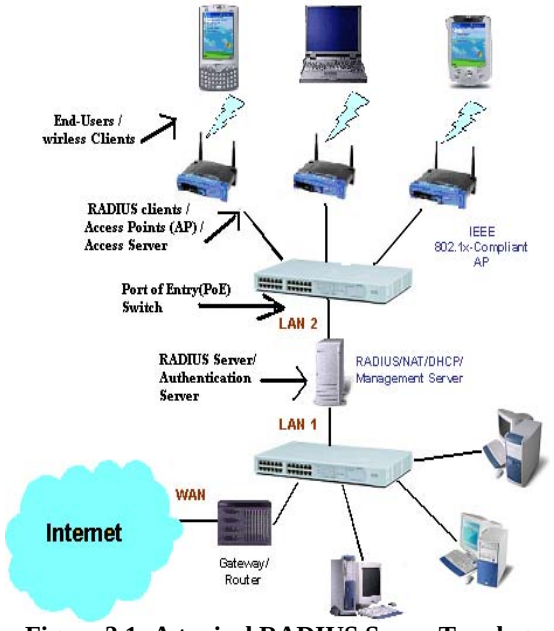

Figure 3.1: A typical RADIUS ServerTopology

Normally, the RADIUS server encapsulates the EAP packets within a standard RADIUS packet, using the EAP-Message attribute, and then transmits them back and forth between the RADIUS Client and the RADIUS server [RFC2869]. The access point then becomes only a pass-through device relaying EAP authentication messages from the wireless Client device to the RADIUS server and vice versa without having to process the packets. This way every new EAP type that is introduced need not be installed at each access point but only at the RADIUS server end. The access point would then behave the same way for each EAP type thus making it extremely flexible.

The RADIUS Client (access point) must however support the negotiation of EAP as an authentication protocol and the passing of EAP messages to a RADIUS server. When

a connection attempt is made, the end user negotiates the use of EAP with the access point. When the user sends an EAP message to the access point, the access point encapsulates the EAP message as a RADIUS message and sends it to its configured RADIUS server. The RADIUS server processes the EAP message and sends a RADIUS-formatted EAP message back to the access point. The access point finally forwards the EAP message to the end user.

IV. Dynamic Extensible Authentication

A. Existing System

There are several extensible authentication methods which has its limitations the table5.1 shows clearly some EAP-methods and its limitations.

B. Proposed system

As analyzed in the above table EAP-TLS provides better security by overcoming some of the limitations in other EAP methods. EAP-TLS can be easily used for device authentication by using digital signed certificates in the device. EAP-TLS is completely password cracking resistant because it does not rely on user passwords. EAP-TLS provides mutual authentication between the supplicant (User) and Authentication server based on X.509 certificates. It eliminates MITM attacks and from rogue AP's. In this proposed system it generates dynamically generates and distributes user based and session based encryption keys to secure connections therefore supplicants(users) identity and password are not revealed. Some of the advantages of the proposed system are[5]:

- Strong wireless security using established standards
- Defends against the weaknesses in WEP encryption, session hijacking, man-in-the-middle attack and dictionary attacks
- Addresses weaknesses in 802.11 (WEP) and 802.1X
- Mutual authentication between client and server
- Easy to deploy and manage
- Proposed system is implemented using JAVA Supports different operating systems and RADIUS servers.

V THE METHOD

Two Server and Client modules were developed in this project. Each module has different packages.

A. Radius packet format

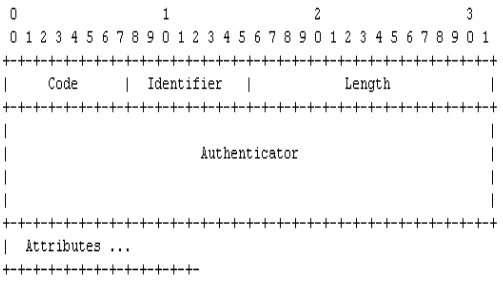

Figure 5.1: Radius packet format

EAP type / Features	MD5	TTLS	PEAP	FAST	LEAP	TLS
Client certificate	no	no	no	no	no	yes
Server Certificate	no	no	yes	no	no	yes
Rogue AP Detection	no	no	no	yes	yes	no
Authentication	One-way	Mutual	Mutual	Mutual	Mutual	Mutual
Ease of Deployment	Easy	Medium	Medium	Medium	Medium	Difficult
WiFi Security	Poor	High	High	High	High (strong password required)	Very high

Table 5.1: EAP-Methods and its limitations.

Code

The Code field is one octet, and identifies the type of RADIUS packet. When a packet is received with an invalid Code field, it is silently discarded.

RADIUS Codes (decimal) are assigned as follows:

1 Access-Request
2 Access-Accept
3 Access-Reject
4 Accounting-Request
5 Accounting-Response
11 Access-Challenge

Identifier

The Identifier field is one octet, and aids in matching requests and replies. The RADIUS server can detect a duplicate request if it has the same client source IP address and source UDP port and Identifier within a short span of time.

Length

The Length field is two octets. It indicates the length of the packet including the Code, Identifier, Length, Authenticator and Attribute fields. The minimum length is 20 and maximum length is 4096.

Authenticator

The Authenticator field is sixteen (16) octets. The most significant octet is transmitted first. This value is used to authenticate the reply from the RADIUS server, and is used in the password hiding algorithm.

B. EAP-TLS Request Packet

Code

1

Identifier

The Identifier field is the one octet and aids in matching responses with requests. The Identifier field must be changed on each Request packet.

Length

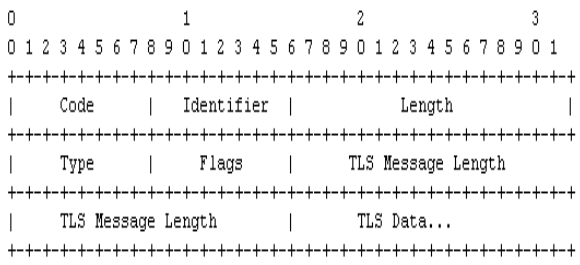

Figure 5.2: EAP-TLS request packet

The Length field is two octets and indicates the length of the EAP packet including the Code, Identifier, Length, Type, and Data fields.

Type

13 -- EAP-TLS

Flags

0 1 2 3 4 5 6 7 8
+-+-+-+-+-+-+-+-+
|L M S R R R R R|
+-+-+-+-+-+-+-+-+
L = Length included
M = More fragments
S = EAP-TLS start
R = Reserved

The L bit (length included) is set to indicate the presence of the four-octet TLS Message Length field, and must be set for the first fragment of a fragmented TLS message or set of messages. The M bit (more fragments) is set on all but the last fragment. The S bit (EAP-TLS start) is set in an EAP-TLS Start message. This differentiates the EAP-TLS Start message from a fragment acknowledgment.

TLS Message Length

The TLS Message Length field is four octets, and is present only if the L bit is set. This field provides the total length of the TLS message or set of messages that is being fragmented.

C. EAP-TLS Response Packet

Code

2

Identifier

The Identifier field is one octet and must match the Identifier field from the corresponding request.

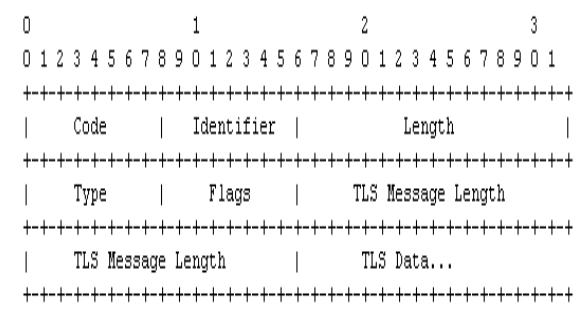

Figure5.3: EAP-TLS response packet

Length

The Length field is two octets and indicates the length of the EAP packet including the Code, Identifier, Length, Type, and Data fields

TLS Message Length

The TLS Message Length field is four octets, and is present only if the L bit is set. This field provides the total length of the TLS message or set of messages that is being fragmented.

TLS data

The TLS data consists of the encapsulated TLS packet in TLS record format.

D. Implementation Architecture of Server

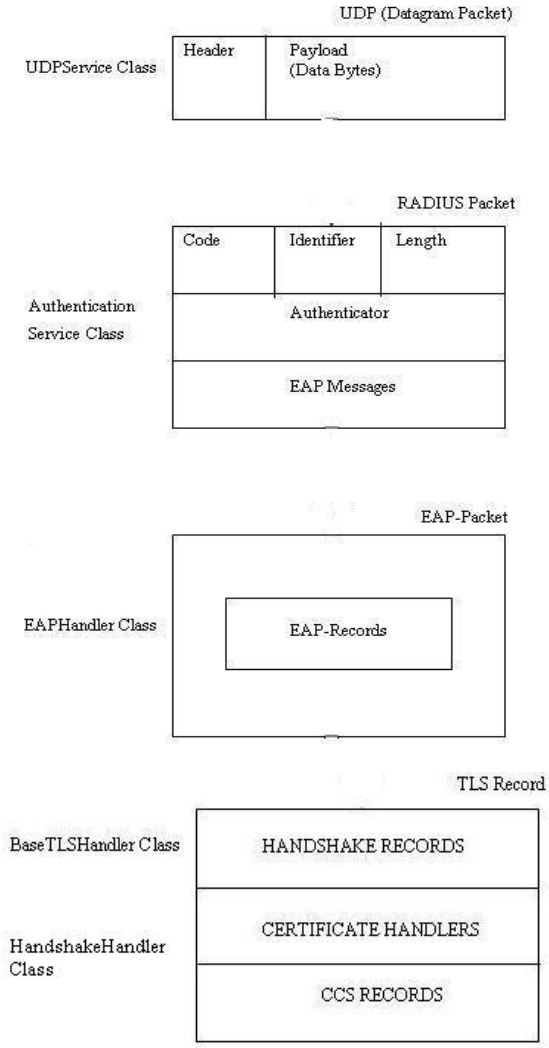

Figure 5.4: Shows the Implementation architecture of Server Module.

E. Implementation Architecture of Client

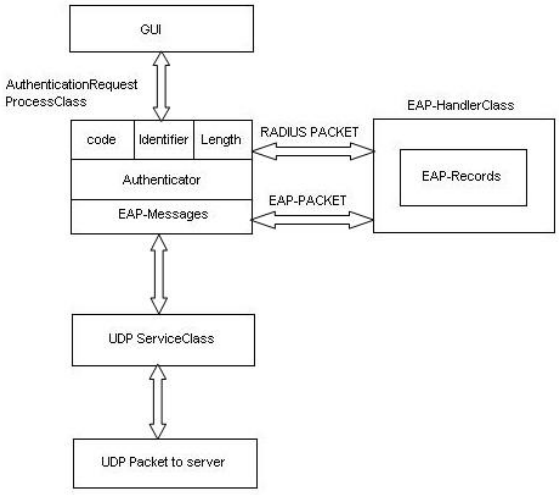

Figure 5.5: shows the implementation architecture of Client Module.

Results

As a proof to the concept a project was developed under same title. Following table gives the test cases for the same.

1	Authentication Validation	All Fields entered with valid data.	Authentication Success message need to be displayed.	Displayed "Authentication Success" message.	Pass
2	Reachablity	Invalid server (IP) address entered.	SocketTimeOut Exception needs to be displayed.	Displayed the "SocketTimeOut Exception".	Pass
3	Validation	When data for mandatory fields are not entered.	Validation false message needs to be displayed.	Displayed Error msg: "User-Id is required".	Pass
4	Shared secret	Invalid Shared secret entered which is not listed at the server end.	Access Reject message has to be shown with Invalid Shared secret reply message.	Displayed "Access Reject" with Invalid Shared secret.	Pass
5	User Test	Invalid username entered which is not listed at the server end.	Access Reject message has to be shown with "User not found"	Displayed "Access Reject" with User not found".	Pass
6	Unknown Client Test	All input are valid but sent from a client which is not listed at the server end.	Error message indicating unknown client.	Display message "Request received from unknown client".	Pass
7	Illegal Port	Any other port other than 1812.	Error message indicating request received through illegal port.	No response from Server.	Pass
8	Certificate Test	Valid certificate	Authentication Success message need to be displayed.	Displayed "Access accept " message	Pass

Conclusion

EAP-TLS provides better security by overcoming some of the limitations in other EAP methods. EAP-TLS can be easily used for device authentication by using digital signed certificates in the device. EAP-TLS is completely password cracking resistant. EAP-TLS provides mutual authentication between the supplicant (User) and Authentication server based on X.509 certificates. It eliminates MITM attacks and from rogue AP's. It dynamically generates and distributes user based and session based encryption keys to secure connections therefore supplicants (users) identity and password are not revealed.

Acknowledgement

We are deeply indebted to all those who have motivated us to prepare this paper.

References

[1] RFC 2716 & 5216 "The EAP-TLS Authentication Protocol".
[2] RFC 3579 "RADIUS and EAP".
[3] RFC 2865 "RADIUS".
[4] Jyh-Cheng Chen and Yu-Ping Wang, "Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience", 2005
[5] Funk, P. and S. Blake-Wilson, "EAP TLS Authentication Protocol (EAP-TLS)", August 2004
[6] Brett Turner, Andrew Woodward Edith Cowan University, "Securing a wireless network with EAP-TLS: perception and realities of its implementation",6th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 1st to 3rd December 2006.
[8] William Stallings ,"Network Security Essentials " Third Edition 2009.
[9][FMS01] Stubblefield, A., Ioannidis, Rubin, A. "Using the Fluhrer, Mantin, and Shamir. Attack to Break WEP".