Analyzing EAP TLS & ERP Protocol with Varying Processor Speed

Bhawna Gupta
N.C.College of Engineering
Israna (Panipat)

Seema Mehla
N.C.College of Engineering
Israna (Panipat)

ABSTRACT

Extensible Authentication Protocol is a generic framework supporting multiple types of authentication methods. In systems where EAP is used for authentication, it is desirable to not repeat the entire EAP exchange with another authenticator. Microsoft has developed EAP TLS which is an authentication protocol based on TLS (Transport Layer Security). Authentication server and client use TLS protocol to negotiate session key. The EAP re-authentication Protocol provides a consistent, method-independent and low-latency re-authentication. It is extension to current EAP mechanism to support intra-domain handoff authentication. This paper analyzed the security cost of EAP TLS & ERP with increased processor speed.

Keywords- ERP; EAP-TLS; EMSK; RADIUS;

I. INTRODUCTION

WEP was the original security mechanism for IEEE 802.11 networks. This was the original encryption standard for wireless. As name implies, this standard was intended to make wireless networks as secure as wired networks. Unfortunately, this never happened as flaws were quickly discovered and exploited A major underlying problem with the existing IEEE 802.11 standard is that the keys are cumbersome to change. If you don't update the WEP keys often, an unauthorized person with a sniffing tool, such as Air Snort or WEP crack, can monitor your network for less than a day and decode the encrypted messages. Wi-Fi Protected Access (WPA) is improvement over WEP. WPA is a trimmed-down version of the 802.11i security standard that was developed by the IEEE 802.11 to replace WEP. WPA Enterprise provides RADIUS based authentication using 802.1x IEEE 802.1X offers an effective framework [10]for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1X makes the use of the Extensible Authentication Protocol (EAP) that defines how authentication messages are to be exchanged [12] between the various network components–clients (supplicants), switches or wireless access points (authenticators), and authentication servers. To optimize the performance of intra-domain re-authentication, some EAP methods have been designed such as the EAP-TLS, which is EAP integration [15] of the TLS protocol supporting either one-way or mutual authentication by using digital certificates. A per-session WEP key could be set up to implement the re-authentication and re-keyed on the peer. However, the problem with EAP-TLS is that it requires the PKI infrastructure to handle certificates, so it is difficult for many private users to deploy. In addition to that the way certificates issued requires multiple rounds of message delivery between the peer and the server. The EAP re-authentication Protocol (ERP), designed by the Handover Keying Working Group of IETF to avoid full EAP exchange to be performed reputedly, we use ERP protocol to authenticate the supplicant locally without communicating with its home Server. This paper is organized as follows: section II introduces the ERP & EAP TLS protocol. Section III introduces EAP TLS Exchange & EAP TLS Security cost computation. Section IV gives ERP Exchange & its security cost computation. Results & discussion are presented in section V. Section VI conclude the paper.

II. EAP TLS & ERP PROTOCOL

Analysis & comparative study conclude that EAP TLS is best among all these methods in terms of Mutual Authentication, Digital Certificate based Authentication, Wi-Fi Security, overall security performance, Immune to dictionary attack, Fast authentication Faster dynamic key generation & it is EAP TLS that have both client & server certificate. Here analyzing the security cost of EAP-re-Authentication & EAP TLS protocol. The ERP proposal is for improving the EAP keying architecture. The aim of ERP is to avoid having the wireless station repeat the entire EAP exchange with every new EAP authenticator it encounters. Master Session Key (EMSK) was derived in initial EAP exchange, the peer and the ER Server use the EMSK to derive a re-authentication Root Key (rRK) for subsequent handover authentication. Thus the ERP specifies a method-independent and efficient re-authentication. The key elements in managing mobility and optimizing efficiency of re-authentication in wireless access mainly focus on the two aspects, (1) the time consumed in the message exchange, (2) the security burden of EAP Server result from computation and verification. We begin with the security analysis along with the description of the EAP-TLS and ERP exchanges.

III. EAP TLS EXCHANGE

EAP-TLS (Transport Level Security) provides strong security by requiring both client and authentication server [7] to be identified and validated. The EAP-TLS is best suited for installations with existing PKI certificate infrastructures. Wireless 802.1X authentication schemes will typically support EAP-TLS to protect the EAP message exchange.

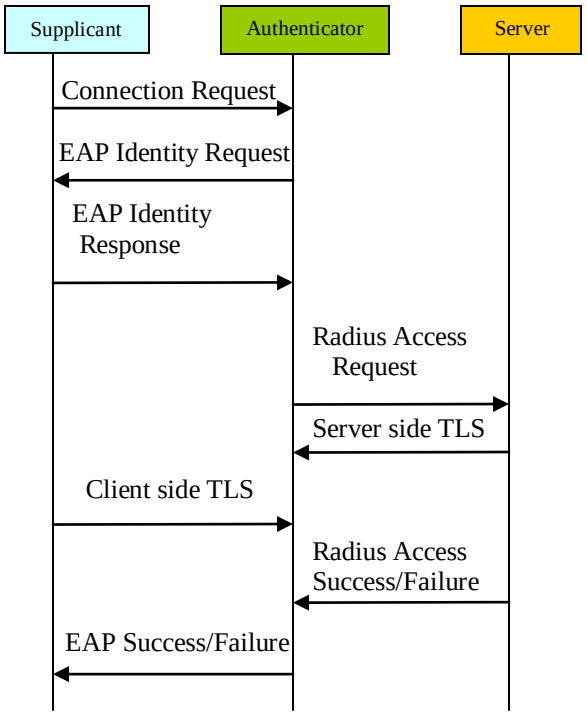

Figure1. EAP TLS Message Flow

Unlike wired networks, wireless networks send their packets over open air making it much easier to capture and intercept unprotected packets. EAP-TLS [16] provides mutual authentication between the client and the authentication server and is very secure. The major drawback of EAP-TLS is requirement for PKI certificates on both the clients and the authentication servers - making roll out and maintenance much more complex.

EAP TLS Security Cost Computation:

EAP-TLS supports two methods [17] for generating keying material. One is RSA encryption based (RSA case) and the other is based on a Diffie Hellman key exchange (DHE case). In the DHE case, the server uses a Server-Certificate of type DHE-RSA or DHE-DSS and following with a Server-Key-Exchange message, including the server's public DH value. Because in RSA case the server uses a certificate of type RSA without sending Server-Key-Exchange, we select this scheme to calculate the security cost of EAP-TLS.RSA method is selected to calculate the security cost of EAP-TLS, as the server uses a certificate of type without sending Server-Key-Exchange. In RSA case, we only consider the time cost of RSA decryption. The time of a 1024-bit modular exponentiation (decryption side of 2048-bit RSA), is about 450,000 CPU cycles on a 64-bit computer [2] which is equivalent to that of the 256 bits modular exponentiation on a 32-bit computer. As the description in, the 256 bit exponentiations costs one of sixteenth of the 1024-bit exponentiations ((256/1024) ^2=1/16), thus we gain the cost of 2048-bit RSA decryption on a 32-bit computer is 450,000×16 = 7,200,000 CPU cycles. The total security cost of EAP-TLS (RSA case), including two times of encryption and one time of decryption, on a Pentium IV-2.6 GHz is about:

Stls = 7,200,000 / 2.6000000000 = 2.76 ms

IV. ERP EXCHANGE

When the supplicant roams to the new network access server it first performs a full EAP exchange with the EAP server. In order to avoid full EAP exchange to be performed reputedly, we use ERP protocol [13] to authenticate the supplicant locally without communicating with its home server. The major difference between the EAP and ERP protocol is the key exchange, ERP first prescribes the generation and deliberation of EMSK, further to generate rRK and rIK for subsequent efficient re-authentication. Then the domain-specified keys generated from DSRK would be used to derive DS-rMSK for efficient re-authentication. That is the establishment of the trust relationship between the Local ER server and the peer via the new Authenticator.

The ERP exchange process is as follows:

i. EAP-Initiate/Re-auth-Start message
ii. EAP-Initiate/Re-auth message between the mobile terminal and the new authenticator.
iii. The server derives rMSK using HMAC algorithms.
iv. The authenticator extracts the rMSK and forwards an EAP-Finish/Re-auth message to the peer.
v. The peer uses sequence number to compute the rMSK as the final step.

ERP Security Cost Computation

a) Security Cost of Message Integrity Calculation:

The EAP-Initiate/Re-auth-Start Packet takes at least one Domain-Name-NAI TLV [13], plus its header; the total Length is

LERS (EAP-Initiate/Re-auth-Start)

= LH + LTLV (Domain-Name-NAI)

= 48 bits + LTLV ≈ 100 bits

The length of the key Name is:

Lkeynam=1-octet (type) +1-octet (length) + value payload

= 16 bits + username length + realm length

= 16bits+16×8bits+ realm length

= 144 bits +L'

≈ 200 bits

Thus the general formula to calculate the length of different EAP /Re-auth packets may be written as [6]:

LRP = LH + LTLV + LAT + LC

= 64 bits + LTLV + 272 bits+8 bits

= 344bits + LTLV

The size of the Diameter Packet [4], LD includes the length of the Diameter Header LDH and the length of the ERP AVP (Attribute value pair)

LD = LDH + LAVP

= 160 bits + LAVP

= 160 bits + 320 bits

= 480 bits

Length of the EAP /Re-auth message:

LD+ Lkeyname = 480bits +200 bits

= 680 bits

Table 1 shows the message packet size & their total length various message that are to sent during ERP process with total CPU cycle for these message packet.

.

Table 1. EAP Re-authentication Message Packet Sizes & CPU cycle of integrity verify

Packet	Total Length (Bits)
EAP-Initiate/Re-auth-Start	100
EAP-Initiate/Re-auth	680
Dim EAP (EAP-Initiate/Re-auth)	1052
Dim EAP (rMSK, EAP-Initiate/Re-auth)	1308
EAP-Finish/Re-auth	680
Total cpu cycles	243974

Upon the receipt of message, the supplicant should demonstrate possession of the rIK by computing the integrity checksum over the EAP-Initiate/Re-auth message

Table 2 key generation during packet

Packet	Key generation
EAP-Initiate/Re-auth-Start	RIK
EAP-Initiate/Re-auth	
Dim EAP (EAP-Initiate/Re-auth)	rMSK
Dim EAP (rMSK, EAP-Initiate/Re-auth)	
EAP-Finish/Re-auth	
Total cpu cycles	243974

Above table shows the keys generated during various message packet for ERP process.

The computation of the checksum can be performed after the analysis of HMAC-SHA256 security algorithm

b) Analysis of HMAC-SHA 256 Security Algorithm:

Secure Hash algorithms SHA256 SHA 256 cannot be used directly as it does not include a secret key [3], therefore combine SHA256 with HMAC, a mechanism to provide integrity check based on a secret key. SHA 256 requires Total 21824 Total Computation & 22084 total of nk times. SHA 256 also needs 210 operations per block for initiation and termination. Thus the total number of operations needed for HMAC-SHA 256 is [1]:

T(nk) = 210 + 22084 nk .

The nk represents the nk -block input data to be encrypted. The required authentication and verification time for HMAC-SHA-256, T (nk, Cp), as a function of the number of input blocks and the processor speed is:

T (nk, Cp) = (210 + 22084nk)/Cp.

nk = N/512 = (8 *Sd + Sp + Ss + K)/ 512.

Where Sd-byte data to be encrypted as an example, N is the N-bit total encryption data, Sp-bit is the length of padding field; Ss-bit is the length of the Size filed and the K-bit denotes the extra appended inner form of the key.

c) Security Cost of Key Generation:

The keys generated in ERP exchange are as follows [19]:

SrIK: rIK label length (Sd) = 40 octets

Length of padding field (Sp) = 1 octet

Length of size field (Ss) = 2 octet

Extra appended bits (K) = 1 octet

Thus the total length of the S is (40+1+2+1) octets = 352 bits. The number of the SHA256 operation nk and the function of the number of input blocks and processor speed T (nk) are:

nk = (1032)/512 ≈2

*T (nk) =210 + 2*22084 = 44378.*

SrMSK: As the rMSK Generation, the length of the S consists of the lengths of the rMSK label, the SEQ and the derived rMSK. The rMSK label as an 8-bit ASCII string, length of 35 bits; The SEQ encoded as a 16-bit number and the "\0" is a NULL octet. The length tag is in length of 16 bits. Thus the length of the S should be:

*S = (35*8+16+16+8) =320 bits.*

Similar as the evaluation of rIK key generating equation, the number of the SHA256 operation nk and the time of rMSK generation SrMSK should be:

nk= 2, SrMSK = T (nk) =44378.

The Security Cost of ERP

The Security cost per step [15] in a network node is given by :

Security cost = time of key generation + Total cpu cycle of Integrity verify

The total security cost in the procedure of Re-authentication according to above section, involves two times of rMSK

generation, five times of verification of authentication tag, is given by:

$$Ss\text{-}erp = 2\times SrMSK + SrIK + Total\ Cpu\ cycle\ of\ Integrity\ verify$$
$$= 3\times 44378/Cp + 243974/Cp$$
$$= 377108/Cp.$$

For same processor speed (Cp) 2.6 GHz , we can calculate the security cost of ERP by using above Eq. & is given by

$$Ss\text{-}erp = 377{,}108 / 2.6000000000 = 0.14\ ms.$$

Thus the security cost of EAP TLS is 19.7 times more than that of ERP.

V. RESULTS & DISCUSSION

Here analyzing the performance of ERP protocol & EAP TLS protocol for IEEE 802.11 standards by comparing the security cost of ERP and EAP-TLS protocols at different processor speeds. Mat lab version 6.5 has been used for system modeling. The size of the message packet in ERP protocol is considered as 100, 680, 1052, 1308 and 680 bits respectively.

The following plot shows that the security cost of ERP & EAP TLS. Table 3 shows the security cost of ERP & EAP TLS with varying processor speed. Security cost of protocol decreases as processor speed increases from MHz to GHz. Figure 2 make it clear that during the authentication process as the speed of processor on which our protocol works is running is slow, then more we have to pay for security that is the security cost is very high on the other side a high speed processor has decreased cost to be pay for security.

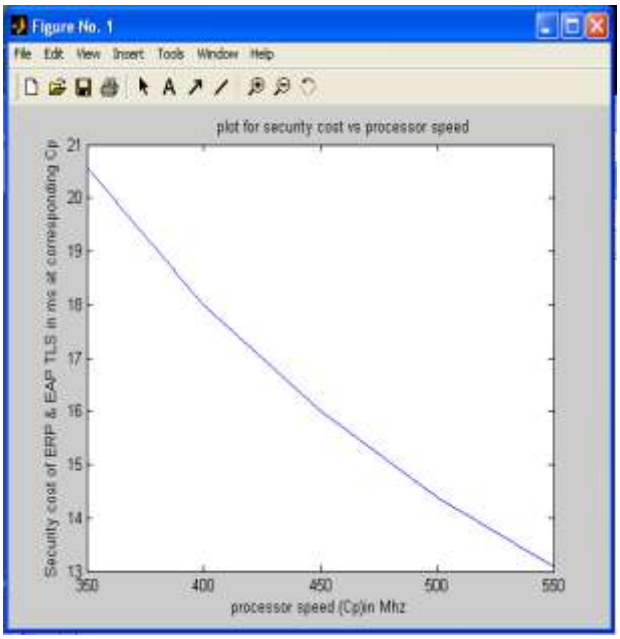

Figure 2 Security Cost of ERP & EAP TLS Protocol

Table 3-processor speed vs security cost

Processor Speed	EAP TLS Security Cost (ms)	ERP Security Cost (ms)
350 MHz	20.57	1.08
400 MHz	18.0	0.94
450 MHz	16.0	0.83
500 MHz	14.4	0.75
550 MHz	13.09	0.68
1GHz	7.2	0.377
1.5 GHz	4.8	0.251
2.0 GHz	3.6	0.188
2.6 GHz	2.76	0.14

Figure 3 analyze the security cost comparison of both ERP & EAP TLS & shows that Security cost of EAP TLS is 19.71 times that of ERP at 2.6 GHz

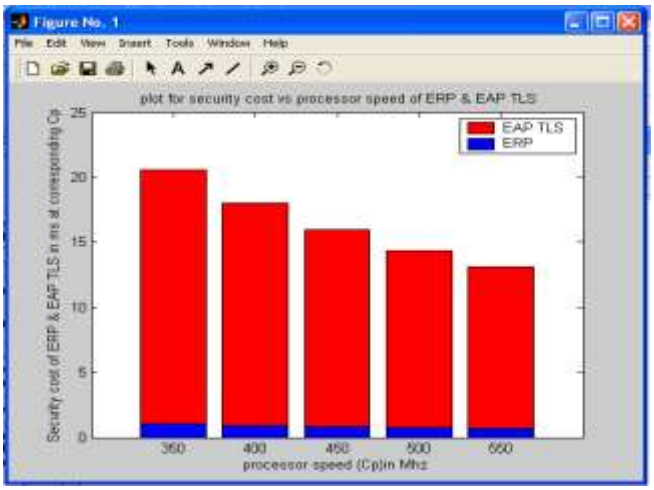

Figure.3 Comparative Security Costs of Both ERP and EAP-TLS Protocol

VI. CONCLUSION

The EAP protocol is a three-party authentication framework, while the ERP protocol is an extension of EAP, which aims to reduce the transmissions and computation costs of EAP. This paper analyzed the efficiency of the ERP protocol and compared it with that of the EAP-TLS protocol (The most important EAP method standardized by the IETF EMU work group). We have computed the security cost of EAP TLS & ERP with processor speed varying from MHZ to GHz. The result shows that the security cost of ERP & EAP TLS is reduced with increased

processor speed & ERP is better than EAP TLS as security cost of EAP TLS protocol is 19.7 times more than that of ERP for 2.6 GHz processor.

REFERENCES

[1] H. Krawczyk, M. Bellare, "HMAC: Keyed-Hashing for Message Authentication," IETF RFC 2104, February 1997

[2] O. Elkeelany, M.M. Matalgah, Performance analysis of IPSec protocol: encryption and authentication, in: IEEE Communications Conference (ICC 2002), 2002, pp. 1164 -1168

[3] Federal Information Processing Standards Publication Specifications for the Secure Hash Standard, August, 2002

[4] H. Orman, Purple Streak Dev., RFC 3766 Determining Strengths For Public Keys Used For Exchanging Symmetric Keys, April 2004

[5] B. Aboba, L. Blunk, J. Vollbrecht, Extensible Authentication Protocol (EAP), IETF RFC 3748 June 2004

[6] P. Calhoun, J. Loughney, E. Guttman, Diameter Base Protocol , IETFRFC 3588, September 2004

[7] P. Eronen, Diameter Extensible Authentication Protocol Application, IETF RFC 4072, August 2005

[8] B. Aboba, M. Beadles, Network Access Identifier (NAI), IETF RFC4282, December 2005

[9] C. Kaufman, Internet Key Exchange (IKEv2) Protocol, RFC 4306, December 2005

[10] T. Clancy, draft-ietf-hokey-reauth-ps-02, "Handover Key Management and Re-authentication Problem Statement", July, 2007

[11] Kaouthar Sethom, "Requirements and Adaptation Solutions for Transparent Handover between Wifi and Bluetooth", Mobile Computing and Communications Review, Volume 8, Number 1, pp. 61-83, San Jose State University, San Jose, CA, USA.

[12] Bernard Aboba, Dan Simon, "Extensible Authentication Protocol(EAP) Key Management Framework", IETF draft-ietf-eap-keying-, November 2007

[13] V. Narayanan, "EAP Extensions for EAP Re--authentication Protocol (ERP)", IETF draft-ietf-hokey-erx-14, March, 2008.

[14]"benchmarks for cryptographic algorithms" unpublishedhttp://www.eskimo.com/~weid/benchmarks.html

ietf-hokey-key-mgm-03, February , 2008.

[15] M. Nakhjiri, Y. Ohba, "Derivation, delivery and management of EAP based keys for handover and re-authentication ", IETF draft

[16] D. Simon,B. Aboba, R. Hurst, RFC 5216 The EAP-TLS Authentication Protocol, March 2008.

[17] Carolin Latze, Ulrich Ultes-Nitsche, Strong Mutual Authentication in a User-Friendly Way in EAP-TLS.

[18] V. Narayanan, L. Dondeti, "Diameter Support for EAP Re-authentication Protocol "IETF draft-dondeti-dime-erp-diameter-01, November, 2007

[19] R Housely, B.Aboba, Guidance for AAA key management, RFC 4296,July 2008