Chapter 5

EAP-CRA for WiMAX, WLAN and 4G LTE Interoperability

E. Sithirasenan, K. Ramezani, S. Kumar and
V. Muthukkumarasamy

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/54837

1. Introduction

Today we are moving into a “post-PC” world! Not many people sit in front of custom built PCs to do their businesses any more. Hand held devices such as iPod Touch, iPhone, Galaxy S3, iPad, Galaxy Tab, Airbook, Notepad etc. are bringing in a new paradigm as to how people use and communicate information. These devices can be thought as a theoretical “black-box”. They are for people who want to use it without wanting to know how they work. Such devices have third generation user interfaces – multi touch, physics and gestures (MPG). They need updates, but the user is not worried of how and where the files are stored. When a new application is installed, the user sees the icon and starts using it. The user is not interested in, what files were installed or where it was installed – there is no file management. The post-PC approach to dealing with software is that it’s discovered on an app store, downloaded with a single touch and deleted with another touch. Updates all come at once from the app store and it all happens behind the scene with minimal user involvement. All this is happening and adopted rapidly because people are able to do a number of things without being restricted to one place. They can download apps, watch movies, listen to news, browse the web etc. while on the move.

However, the mobility of these post-PC devices is restricted to some extent due to the limitations in wireless data connectivity. A wireless device at home should preferably get its data connectivity through the wireless router, while on the move from the 3G or 4G network and while at work from the office wireless network. To achieve this interoperability the wireless devices must be recognized by the various networks as it roams from one network to another. Integration of wireless networks has its own advantages and disadvantages. One type of network that is suitable for a particular application may not be appropriate for another. A security mechanism that is effective in one environment may not be effective in the other. There can be situations where different types of networks coexist in one geographical area. However, due to the inherent nature of the wireless communications, wireless networks encounter numerous security problems compared to its wired counterpart. The most significant of these is the first time association. Whether it is a WLAN [1], WiMAX [2] or a 4G LTE [3], all wireless networks will have this setback. The lack of physical connectivity (anchor-attachment) from the wireless device to the network makes the wireless network more vulnerable and hard to protect against authenticity, confidentiality, integrity and availability threats [4][5]. Hence, to overcome this first time association problem wireless devices adopt a range of different techniques.

The Robust Security Network Association (RSNA) proposed in IEEE 802.11i [6] has emerged as the most popular method to counter the first time association problem. The RSNA technique is widely used in both WLANs and WiMAX. Although IEEE 802.11i security architecture offers sufficient protection to the wireless environment, it is up to the implementer to guarantee that all issues are addressed and the appropriate security measures are implemented for secure operation. A single incorrectly configured station could lead the way for a cowardly attack and expose the entire organizational network [7][8].

Notwithstanding the configuration issues, RSNA is the most preferred first time association method for wireless networks. The use of IEEE 802.1x port based access control [9] makes it more flexible for mutual authentication and key distribution. However, RSNA does not provide options for coordinated authentication in a heterogeneous network environment. This results in the wireless users having to use different credentials to authenticate with different wireless networks. Hence, a wireless device will have to repeatedly authenticate itself as it roams from one network to another operators' network, be it the same type of network or different. Therefore, a Coordinated Robust Authentication (CRA) Mechanism with the ability to use a single set of credentials with any network, wireless or wired would be of immense significance to both network users and administrators. In this chapter we present technical details of CRA together with some experimental results. However, before illustrating the details of CRA, we first present an overview of RSNA.

1.1. Robust security network association

The IEEE 802.11i standard defines two classes of security framework for IEEE 802.11 WLANs: RSN and pre-RSN. A station is called RSN-capable equipment if it is capable of creating RSN associations (RSNA). Otherwise, it is a pre-RSN equipment. The network that only allows RSNA with RSN-capable equipments is called an RSN security framework. The major difference between RSNA and pre-RSNA is the 4-way handshake. If the 4-way handshake is not included in the authentication / association procedures, stations are said to use pre-RSNA. The RSN, in addition to enhancing the security in pre-RSN defines a number of key management procedures for IEEE 802.11 networks. It also enhances the authentication and encryption mechanisms from the pre-RSN. The enhanced features of RSN are as follows:

Authentication Enhancement: IEEE 802.11i utilizes IEEE 802.1X for its authentication and key management services. The IEEE 802.1X incorporates two components namely, (a) *IEEE 802.1X Port* and (b) *Authentication Server (AS)* into the IEEE 802.11 architecture. The IEEE 802.1X port represents the association between two peers as shown in Figure 1. There is a one-to-one mapping between IEEE 802.1X Port and association.

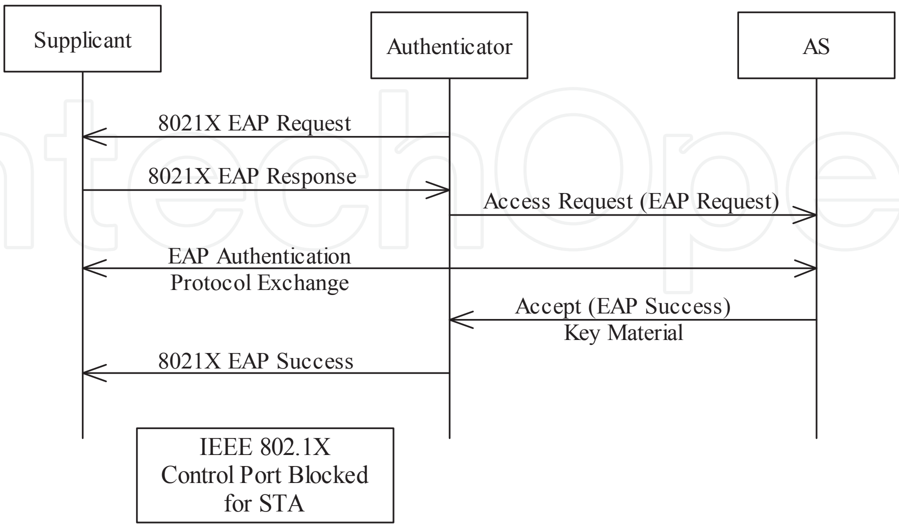

Figure 1. IEEE 802.1X EAP Authentication

Key Management and Establishment: Two ways to support key distribution are introduced in IEEE 802.11i: *manual key management* and *automatic key management.* Manual key management requires the administrator to manually configure the key. The automatic key management is available only in RSNA. It relies on IEEE 802.1X to support key management services. More specifically, the 4-way handshake is used to establish each transient key for packet transmission as in Figure 2.

Encryption Enhancement: In order to enhance confidentiality, two advanced cryptographic algorithms are developed: Counter-Mode/CBC-MAC Protocol (CCMP) and Temporal Key Integrity Protocol (TKIP). In RSN, CCMP is mandatory. TKIP is optional and is recommended only to patch any pre-RSN equipment.

During the initial security association between a station (STA) and an access point (AP), the STA selects an authorized Extended Service Set (ESS) by selecting among APs that advertise an appropriate Service Set ID (SSID). The STA then uses IEEE 802.11 Open System authentication followed by association to the chosen AP. Negotiation of security parameters takes place during association. Next, the AP's Authenticator or the STA's Supplicant initiates IEEE 802.1X authentication. The Extensible Authentication Protocol (EAP) used by IEEE 802.1X will support mutual authentication, as the STA needs assurance that the AP is a legitimate Access Point.

The last step is the key management. The authentication process creates cryptographic keys shared between the IEEE 802.1X AS and the STA. The AS transfers these keys to the AP, and the AP and STA use one key confirmation handshake, called the 4-Way Handshake, to complete security association establishment. The key confirmation handshake indicates when the link has been secured by the keys and is ready to allow normal data traffic.

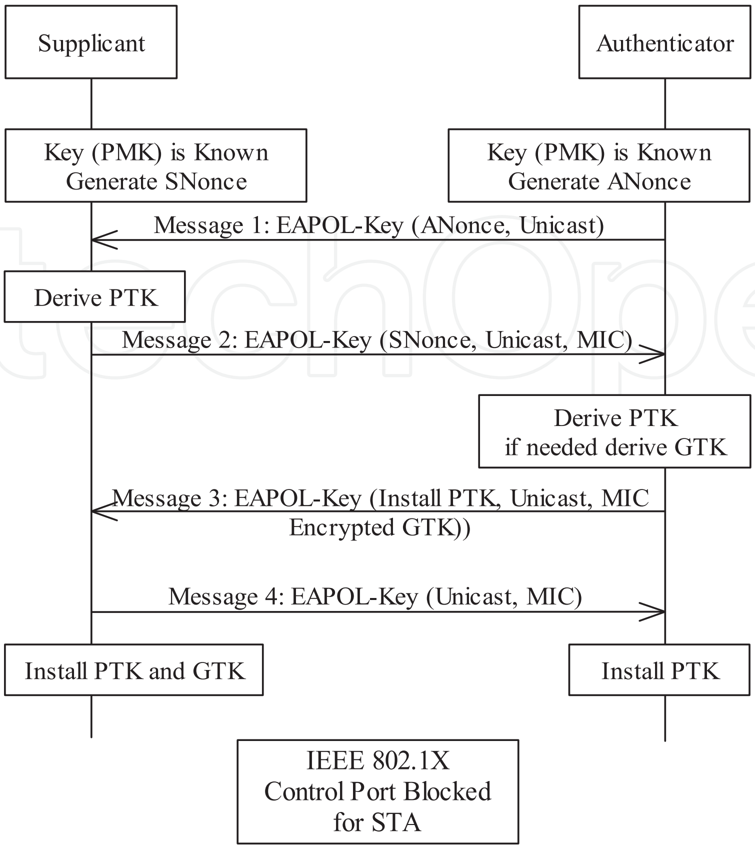

Figure 2. Establishing pairwise & group keys [6]

In the case of roaming, an STA requesting (re)association followed by IEEE 802.1X or pre-shared key authentication, the STA repeats the same actions as for an initial contact association, but its Supplicant also deletes the PTK when it roams from the old AP. The STA's Supplicant also deletes the PTKSA when it disassociates / de-authenticates from all basic service set identifiers in the ESS. An STA already associated with the ESS can request its IEEE 802.1X Supplicant to authenticate with a new AP before associating to that new AP. The normal operation of the DS via the old AP provides communication between the STA and the new AP.

2. Existing methods for integrating wireless networks

Iyer et al. [10] claim that WLAN and WiMAX are particularly interesting in their ability towards mobile data oriented networking. They confirm that a scheme enabling mobility across these two would provide several advantages to end-users, wireless operators as well as Wireless Internet Service Providers (WISP). Further, they propose a technique with a common WLAN/WiMAX mobility service agent for use across WLAN and WiMAX access. By incorporating an acceptable mapping mechanism between WLAN and WiMAX, they interface a WLAN Access Point with the WiMAX Access Service Network (ASN) gateway. The mapping function inside WLAN access point maps all 802.11 events to the WiMAX events. For example the event association request will be mapped to WIMAX pre-attachment request.

In their architecture the problem of handling mobility across WLAN and WiMAX boils down to the problem of handling mobility across WiMAX base stations that already have concrete solutions. Also, the mapping function consumes 1.82 seconds for EAP-TLS authentication in comparison to few milliseconds in CRA. Further, their proposed architecture enables the same IP address to be used across both the WLAN and the WiMAX network interfaces, and keeps it seamless from an application perspective.

Distributed authentication scheme proposed by Machiraju et al. [11] relies on Base Stations (BS) to collectively store authentication information. To achieve the goal of single point of access they introduce the notion of tokens. The token contains the identity and other information regarding the user. Each mobile user has exactly one token that is stored at the base station where the mobile user is receiving service. When the mobile user moves between base stations, its token moves along with the user, thus, eliminating the need to maintain costly infrastructure required by traditional centralized scheme. They assert two main disadvantages of centralized authentication methods. Firstly, a server must be available. Without a server the authentication process cannot be completed. Secondly, there must be a highly reliable backhaul. The latter is due to the authentication process creating a large volume of traffic, usually of a higher priority than normal traffic. They further emphasize that their scheme is optimized for mobility-induced handover re-authentication and, thereby reducing the authentication overheads. This study however, does not clarify how the base stations will initiate contact with each other. The security approach to establish a secure connection between the BS is not determined. Moreover the details to establish trust between base stations and actions taken in case of base stations being compromised are not provided. The capabilities required to perform the expected functionality of a BS are not addressed.

The EAP-FAMOS authentication method developed by Almus et at. [12] use the Kerberos based authentication in the existing EAP framework. It allows secure and true session mobility and requires the use of another EAP method, only for the initial authentication. It uses the keying material delivered by the other EAP method during the initial authentication for its Kerberos-based solution for fast re-authentication. Mobility is based on Mobile IPv4 and a sophisticated handover supported by a so-called Residential Gateway together with a Mobility Broker located in the ISP's backend network. Their performance studies show that Wi-Fi technology can be used in mobile scenarios where moving objects are limited to speeds below 15kmh. Further, they state that applications requiring very low delay and allowing only very short service interruptions can be supported by their technique.

OSNP is another EAP method based on Kerberos proposed by Huang et al. [13]. The protocol provides intra-domain and inter-domain authentication to a peer that already has its security association with the home network. The authors have proposed a hierarchal design for KDC servers with the Root KDC responsible for providing directory service to other KDC servers. In case of a request to a particular network other than the peer's Home network, the authentication server in the new network will obtain the authenticity of the peer from the home KDC. Although the authors suggest a quick password based authentication and roaming mechanism, they fail to provide details of the hierarchical design of KDC servers and the agreement between them. Moreover, all servers share a group key and in case of a key compromise, access points can masquerade as legitimate authenticators.

Apart from the high administrative costs in Kerberos based methods; their solution is mainly targeted at specific wireless networks and authentication mechanisms. Wireless service providers use different authentication schemes on their diverse types of wireless networks. For example, a WiMAX service provider may use the EAP-TLS authentication scheme on their custom Authentication Authorization and Accounting (AAA) server, whereas corporate entities may want to use EAP-TTLS authentication mechanism facilitating the use of their existing authentication databases such as Active Directory, LDAP, and SQL. Hence, for convergence of wireless networks it is significant to develop an authentication mechanism that is versatile and simple so that it can be effectively used in any type of wireless network.

Narayanan et al. [14] propose ERP, an extension to the EAP framework and an EAP key hierarchy to support Re-authentication. As specified in RSNA, MSK is generated on successful completion of the authentication phase (phase 2 of RSNA). Subsequently MSK is passed to the authenticator to generate the TSK (phase 3 of RSNA). The TSK is then used for data encryption between the supplicant and the authenticator. However, the EAP framework proposed by Narayanan et al. suggests two additional keys to be derived by all EAP methods: the Master Session Key (MSK) and the Extended MSK (EMSK) which forms the EAP key hierarchy. They make use of the EMSK for re-authentication and successive key derivations.

ERP defines two new EAP messages EAP-Initiate and EAP-Finish to facilitate Re-authentication in two round trip messages. At the time of the initial EAP exchange, the peer and the server derive an EMSK along with the MSK. EMSK is used to derive a re-authentication Root Key (rRK). The rRK can also be derived from Domain-Specific Root Key (DSRK), which itself is derived from the EMSK. Further, a re-authentication Integrity Key (rIK) is derived from the rRK; the supplicant and the authentication server use the rIK to provide proof of possession while performing an ERP exchange. After verifying proof of possession and successful authentication, re-authentication MSK (rMSK) from the rRK is derived. rMSk is treated similar to MSK obtained during normal EAP authentication i.e. to generate TSK [15].

Apart from the few modifications to the EAP protocol due to the introduction of two new EAP codes, ERP integrates with the existing EAP framework very well. To demonstrate the possession, supplicant uses rIK to compute the integrity checksum over the EAP-Initiate message. The algorithm used to compute integrity checksum is selected by the peer and in case of server's policy does not allow the use of cipher suite selected by the peer; the server sends a list of acceptable cipher suites in the EAP-Finish / Re-auth message. In this case the peer has to re-start the ERP process by sending the EAP-Initiate message and the integrity checksum using the acceptable cipher suites. Furthermore ERP also recommends use of IPsec or TLS to protect the keying materials in transit. However, EAP-ERP requires a full EAP authentication at first when a user enters a foreign network. Further, if one supplicant for any reason has not been able to extract domain name of the foreign network then it should solicit it from its Home server, this can result in long authentication delays.

Increasing use of Mobile devices and new data capabilities on these devices suggest more attention for fast and secure handover. Authentication mechanisms such as EAP-AKA and EAP-SIM facilitate handover and re-authentication for 3GPP interworking.

3. Coordinated Robust Authentication

The principal notion behind the Coordinated Robust Authentication (CRA) [16] mechanism is that every wireless device will primarily be associated with one wireless network, which can be referred to as its HOME network. The credentials used by a wireless device to associate with its HOME network are assumed to be robust and specific to that network. Therefore, a wireless device must be able to use its authority in the HOME network to reliably associate with any other FOREIGN network. In this context, the AAA server that authorizes the wireless device in its home network is called as the HOME AAA Server and the AAA server in a foreign network is called as the FOREIGN AAA Server. Hence, in CRA, a wireless device will require only one set of credentials that it uses to access the home network to access any type of foreign networks. CRA considers both different types of networks and different authentication mechanisms that may be specific and effective to that type of network.

Therefore, in this mechanism a wireless device will deal with one HOME network and a number of FOREIGN networks. It also assumes that the security mechanism used in the HOME network is the most effective that can be adapted to the type of wireless devices used in the network. Further, it is assumed that the HOME AAA server will have pre-arranged agreements with the FOREIGN AAA servers for secure communications by other means such as IPSec, SSL etc.

Figure 3 outlines the messages exchanged in CRA. As in the RSNA, the CRA also includes a discovery phase that comprises of the six 802.11 open system association messages. During this phase a wireless device that is in the FOREIGN network will advertise that it is capable of EAP-CRA together with other allowed EAP methods. Hence, an authenticator in the FOREIGN network can initiate EAP-CRA if it is capable of managing it. Once they both agree on the EAP-CRA mechanism, the authenticator can initiate the EAP-CRA by sending the EAP Request / Identity message to the supplicant (message 7 in Figure 3). The supplicant in return will reply with the EAP Response / Identity message (message 8). The Response / Identity message is passed to the FOREIGN AAA server as a RADIUS Access Request message. At this stage unlike in the other EAP authentication methods the AAA server will pass the Access Request message to the relevant HOME AAA server for validation. If the HOME AAA server successfully validates the Identity information sent by the wireless device, it then responds with an Access Accept message with the necessary keying material to the FOREIGN AAA server. The keying material, in-turn, is passed to the authenticator with the RADIUS Access Accept message. The authenticator can then use the keying material to initiate the 4-way handshake process to generate the TSK. Further details of the CRA protocol are explained in the next section.

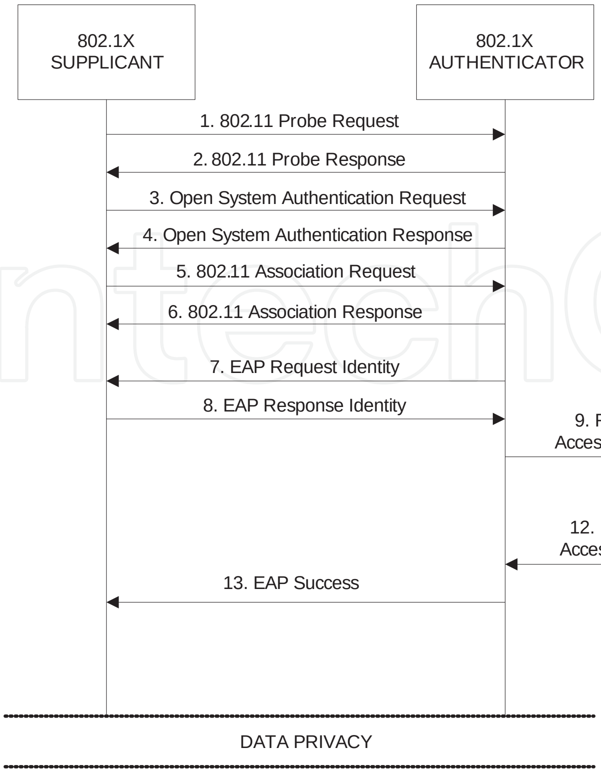

Figure 3. Coordinated authentication message exchange

3.1. The EAP-CRA protocol

With regard to mutual authentication EAP-CRA uses RADIUS servers as suggested in IEEE 802.1x [17]. RADIUS protocol exhibits better performance compared to other mutual authentication protocols [18]. EAP-CRA offers direct communication between radius servers by pre-arranged agreement or the servers could find each other dynamically. In case the RADIUS servers do not have a pre-arranged agreement then they can use their CA-signed PKI certificates to ascertain trust between servers.

All AAA servers that participate in the EAP-CRA must have some pre-arranged agreement for secure communication. Assuming that all AAA Servers that participate in the EAP-CRA are in possession of their CA-signed PKI certificates, the CRA protocol uses the CA-signed PKI certificates to communicate between the FOREIGN and the HOME AAA servers. However, other options for secure communications such as a virtual private network (VPN) or SSL can also be used. In the protocol details shown in Figure 4, CRA uses the already available CA-signed PKI certificates of the FOREIGN and the HOME AAA servers for secure communication. Message 3 is encrypted using the private key of the FOREIGN AAA server ($E_{KP_F}[HostName, E_{KU_H}[EMSKname, SeqNo.]]$) and message 4 is encrypted using the public key of the FOREIGN AAA server ($E_{KU_F}[DSRK]$). However, in Figure 4, we have left the issue of secure communication between the FOREIGN and the HOME AAA server open, to confirm that other options are possible.

According to the EAP-CRA protocol, in response to the EAP-CRA Request Identity message (message 1 in Figure 4), the supplicant sends an EAP Response message with its *Identity* (EMSKname and Sequence number) encrypted with the public key of the HOME AAA server (message 2 in Figure 4) along with the unencrypted host name of the HOME AAA server. EMSKname is used to identify the corresponding EMSK and Sequence Number for Replay protection by the Home AAA server. The authenticator, having received the encrypted *Identity* will pass it to the FOREIGN AAA server as it is. The FOREIGN AAA server uses the fully qualified *Host Name* provided in EAP-CRA Response message to determine the Home AAA server. The FOREIGN AAA server will append its *Domain name* to the received message (EAP-CRA Response) and pass it to the HOME AAA server using the secure method described above (message 3).

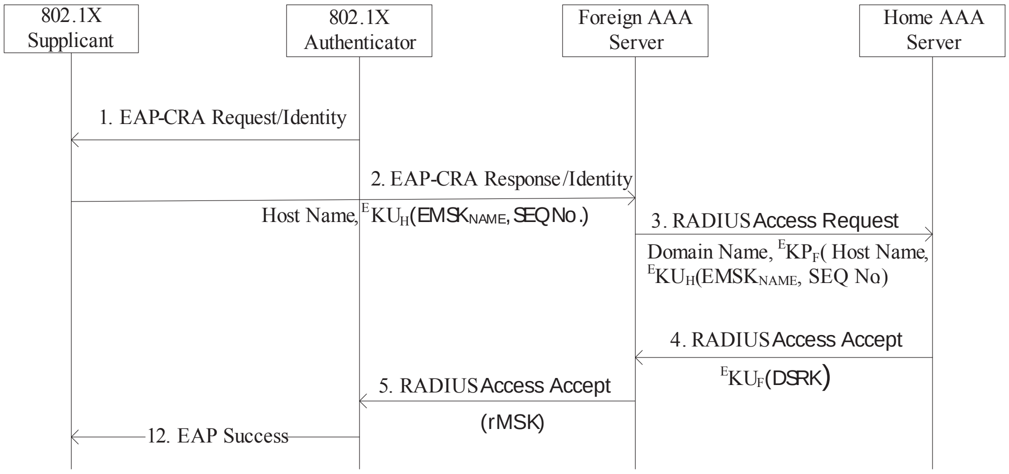

Figure 4. Coordinated Robust Authentication (CRA) Protocol.

The HOME AAA server will then have to do a double decryption to find the identity of the HOME wireless device. If the wireless device is positively identified, the HOME AAA server calculates *DSRK* (Domain Specific Re-authentication key). DRSK is calculated using *Domain Name* as an optional data in the key derivation specified in [15]. HOME AAA server will then send the *DSRK* to the FOREIGN AAA server after encrypting the message using the public key of the FOREIGN AAA server (message 4). This process is illustrated in Figure 5. The FOREIGN AAA server can use its private key to decrypt the received message to discover the *DSRK* and generate *rMSK* (Re-authentication Master Session Key). rMSK is calculated using a sequence number as an optional data specified in [14]. The *rMSK* can then be transferred to the authenticator with the RADIUS Access Accept message (message 5 in Figure 4). Finally the authenticator sends the EAP success message to the wireless device indicating the completion of the CRA authentication and the beginning of the key distribution phase.

Two sequence numbers, one with HOME AAA server and one with FOREIGN AAA server is maintained for replay protection of EAP-CRA messages. The sequence number maintained by the supplicant and HOME AAA server is initialized to zero on the generation of EMSK. The server sets the expected sequence number to the received sequence number plus one on every successful Re-authentication request i.e. on generation of DSRK. Similarly the supplicant and the FOREIGN AAA server maintain a sequence number with the generation of rMSK until the supplicant is in the FOREIGN AAA server's domain.

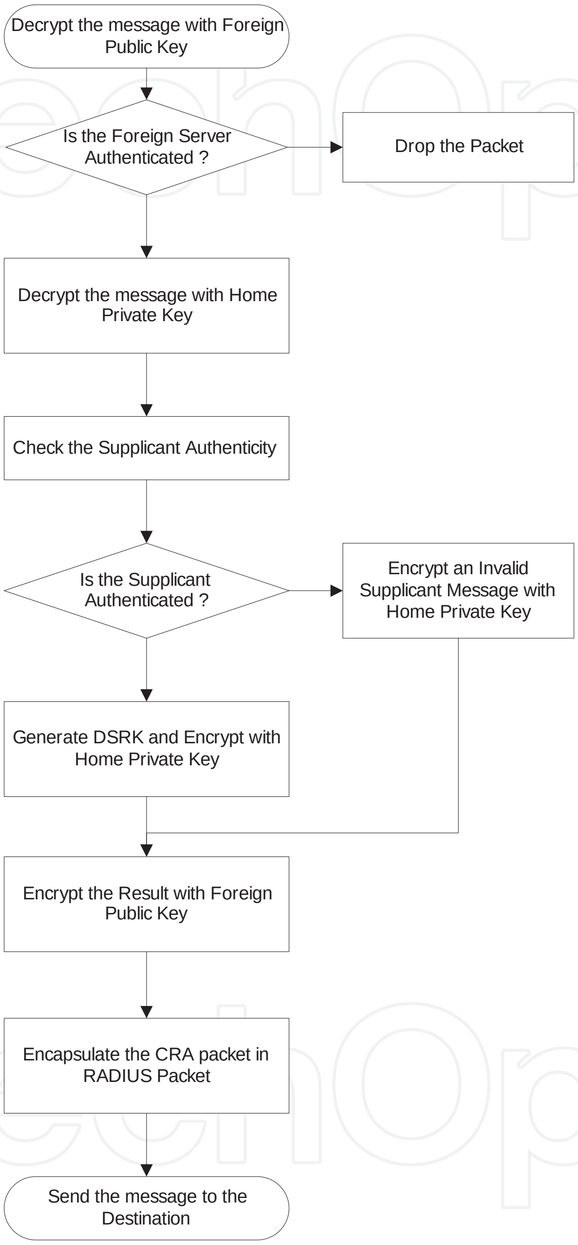
Decrypt the message with Foreign Public Key
Is the Foreign Server Authenticated ?
Drop the Packet
Decrypt the message with Home Private Key
Check the Supplicant Authenticity
Is the Supplicant Authenticated ?
Encrypt an Invalid Supplicant Message with Home Private Key
Generate DSRK and Encrypt with Home Private Key
Encrypt the Result with Foreign Public Key
Encapsulate the CRA packet in RADIUS Packet
Send the message to the Destination

Figure 5. EAP-CRA on Home Server

On receiving the EAP success message, the peer generates rMSK independently leading to the key distribution phase. The key distribution phase will be similar to that of the RSNA where the supplicant and the authenticator will use the MSK to derive TSK. Once the Temporary Session keys (TSK) are derived normal data communication can commence. In the next section we discuss the server side communication of the CRA authentication mechanism.

3.2. Extentions to RADIUS

EAP-CRA uses RADIUS as the transportation protocol between the Home and Foreign servers. However the RADIUS protocol is a client-server protocol. The RADIUS server, when forwarding the authentication packet to another RADIUS server, designates the sender as client. Hence, the foreign server's only responsibility is to fulfill the role of a proxy server and to forward the RADIUS packets to the Home server. EAP-CRA takes advantage of RADIUS communication and encapsulates the EAP-CRA messages inside the RADIUS packets. There are two viable approaches to designing the security methods that were discussed in the previous section.

The first approach is to implement the security features inside the attribute field of the RADIUS packet (Table 1). The attribute field of each RADIUS Packet includes at least three fields that enable the RADIUS packet to carry EAP messages or other information for Dial in user. The attribute field can be used to encapsulate EAP-CRA messages inside the RADIUS packet. Extensions to RADIUS protocol so far proposed have been for the purpose of modifying or creating new attributes such as EAP or apple extensions for RADIUS, each of which has particular attributes.

0 0	1	2	3	4	5	6	7	8	9	1 0	1	2	3	4	5	6	7	8	9	2 0	1	2	3
Type								Length								Value …							

Table 1. Attributes in a RADIUS packet

Type 79 is for EAP messages and 92-191 are Unused. If the value is string or text type then the length can be from 1 to 253 octets. Therefore the type value can be between 92 to 191 octets for the EAP method. The type of the value will be string and as with other EAP methods data is encapsulated inside the RADIUS packet. The foreign server can encapsulate the encrypted message inside the RADIUS packet, so that the home server must first decrypt the message and then respond by a proper RADIUS message to the foreign server.

The second approach is to use a dependent VPN over a SSL connection between the two servers prior to RADIUS communication. The RADIUS packets can then be sent in a secure channel. However, EAP-CRA does not use this method because it entails extra network administration. It also creates a connection delay prior to the EAP-CRA message transmission. Also, the use of PKI actually provides a more secure channel by which the EAP-CRA message can be sent and received.

3.2.1. EAP-CRA message and process details

The proposed EAP-CRA packet is depicted in Table 2. The reasons for designing each of the fields are illustrated based on the associated requirements. The fields are transmitted from left to right. The first influencing factor of EAP-CRA is that it is based on the EAP protocol.

Therefore, the fields, code, identifier and length are inherited from an EAP structure. The explanation of each field is listed below.

00	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
Code								Identifier								Length of CRA															
Type								Flags								CRA Message Length															
CRA Message Length																CRA Data …															

Table 2. CRA Packet

The Code field is one octet and identifies the type of EAP packet. EAP Codes are assigned as 1 for Request, 2 for Response, 3 for Success and 4 for Failure. The Identifier field is one octet and aids in matching responses with requests. The Length field is two octets and indicates the length of the EAP packet including the Code, Identifier, Length and Data fields. Octets outside the range of the Length field should be treated as Data Link Layer padding and should be ignored on reception. The Flags field includes the following fields:

0	1	2	3	4	5	6	7
L	M	S	T	R	R	R	R

L = Length included, M = More fragments, S = EAP-CRA start, R = Reserved, T = Source Type

Table 3. Add Caption

3.2.2. Two kinds of RADIUS packets in EAP-CRA

In EAP-CRA, RADIUS packets are divided into two categories, based on their content. The first category includes those messages sent from an access point to the foreign server and the second type is those exchanged between a Home and Foreign server. In the first scenario, the supplicant encrypts the EAP-CRA message using the Home server public key and sends it to the foreign server. Between the home server and the client, the authenticator encapsulates the message inside a RADIUS packet and sends it to the foreign server. On the other hand, when the two servers are in communication with each other they sign the EAP-CRA message first using their own private key and then by encrypting the message using the other server's public key. Therefore, the content of the RADIUS packets differ depending on whether they are received from an authenticator or from an authentication server. The field T in the fragmentation field is for source type of the packet. If the packet is from or is sent to an authenticator then the value will be set to 0. Otherwise, if the source is a server, then the value will be set to 1.

Retry behavior: It is possible during peer communication that a response will not occur within the expected time. In which case, there must be a way to specify how many messages will be sent to make sure that another peer is not present. The time to resend the message is another parameter which needs to be determined. The exact number for the time and trials will be decided in the actual implementation and depends on the protocol process time, line traffic and other unforeseen factors. One of the issues present in retry is the duplicate packets which must be handled by the receiving peer. Three retries will be performed, forming the base configuration for the EAP-CRA.

Fragmentation: EAP-CRA message may span multiple EAP-packets due to the multiple public and private key encryptions; hence there must be a method, to be engineered in the servers, for handling the fragmentation. As a base for work on the fragmentation, the length of the TLS record can be up to 16384 octets, while the TLS message may be 16 MB if it carries the PKI certificate of a server. However, to protect against denial of service attacks and reassembly lockup there must be maximum size set for the group of the fragmented messages. An example can be seen in what was implemented for EAP-TLS[19]. The exact numbers will be determined during implementation of the protocol, and will reveal the average length of long EAP-CRA messages. For the purposes of initial configuration, this number can be borrowed from EAP-TLS which is 64 KB.

Since EAP is an uncomplicated ACK-NAK protocol, fragmentation support can be provided according to a relatively simple process. Damage or loss of fragments during transit is an inevitable risk for any communication. In EAP, these fragments will be retransmitted, and because sequencing information is included in EAP's identifier field, a fragment offset field like that of IPv4 is not necessary.

EAP-CRA fragmentation support will be provided by adding flag fields to the EAP-CRA packets inside the EAP-Response and EAP-Request. Flags include the Length (L), More fragments (M), and Start (S) bits. The L flag indicates the presence of the four octet Message Length field. It *must* be set in the first piece of a fragmented EAP-CRA message or set of messages. The M flag will be set in all except the last fragment showing that there are more frames to follow. The S flag will only be for the EAP-CRA start message sent from the EAP server to the peer. The T flag refers to the source type of the EAP-CRA message; whether it is coming from an 802.1x authenticator or from an authentication server. If there is a fragmented message, both server and the other peer must acknowledge the receipt of a packet with the flag set to M. The response can be an empty message to the other peer showing that the message has not been received.

3.3. Experiments

For our experiments we setup three different scenarios to compare the time taken to authenticate a user. Edu-roaming, EAP-CRA and direct authentication with a single RADIUS authentication server were considered. RADIUS servers were installed on Windows 2003 Server standard edition and all platforms had 2 GB RAM and 2GHz dual core CPU.

Microsoft Internet Authentication Service (IAS) with Microsoft EAP-PEAP was used in these experiments. IAS is the Microsoft implementation of a Remote Authentication Dial-In User Service (RADIUS) server and proxy in Windows Server 2003. As a RADIUS server, IAS performs centralized connection authentication, authorization and accounting for many types of network access including wireless and VPN connections. As a proxy, the IAS forwards authentication and accounting messages to other RADIUS servers.

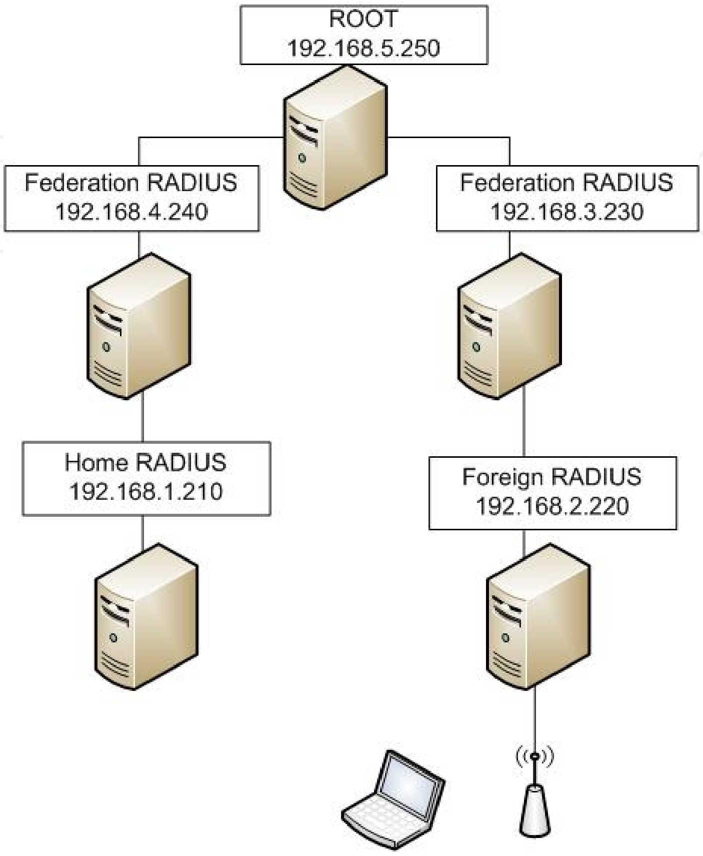

Figure 6. Experimental Edu-roam Setup on LAN

To start with fair baselines both EAP-CRA and Edu-roaming were implemented in LAN but in different IP subnets. Moreover to magnify the delay of authentication for Edu-roaming another setup on Internet was also implemented. The first topology is the Edu-roaming model. Since this is a proprietary model it was implemented on five Microsoft IAS that was installed on the Java virtual box. Because the Edu-roaming has federation level RADIUS servers and one root RADIUS server, we implemented five RADIUS servers in all. Two of the RADIUS servers were for the home and the foreign networks, two as the federation level RADIUS servers and the last one as the Root authentication server. Figure 6 shows the topology for Edu-roaming that was implemented by us.

The second scenario was an implementation of Edu-roaming and EAP-CRA servers on the Internet. Five servers were installed at various remote sites in Brisbane Australia. In all scenarios, the time difference between the first RADIUS request message and the last RADIUS accept message was used for comparing the time taken for authentication. Tables 4 and 5 lists the average times obtained on the LAN and Internet implementations over forty different trials.

Topology	Edu-roam	EAP-CRA	Direct
Average Time (ms)	259	148	119

Table 4. Average Authentication Time on LAN

Topology	Edu-roam	EAP-CRA
Average Time (ms)	4176	750

Table 5. Average Authentication Time on Internet

According to Table 1 there is a 111 milliseconds time difference in the authentication times between Edu-roaming and the EAP-CRA. As explained earlier the EAP-CRA directly communicates with the foreign RADIUS server. Moreover, the difference in authentication times between the CRA approach and direct authentication with the RADIUS server is 29 milliseconds. Table 5 shows the authentication times over the Internet. Here, the RADIUS servers are located at different locations and are connected over the Internet. In this case there is a significant difference in authentication times between Edu-roaming and EAP-CRA approaches. The Edu-roaming approach is almost three times slower than the EAP-CRA approach in this case.

3.4. Discussion

Figure 7 confirms the potential of the EAP-CRA approach compared to the other methods. The main advantage of the EAP-CRA authentication mechanism is the use of only two messages to authenticate a wireless device in a FOREIGN network. Although the time taken between the FOREIGN AAA server and the HOME AAA server may vary depending on the traffic and/ or capacity of the wired network, the use of only two messages in a FOREIGN network makes CRA authentication mechanism very much reliable compared to other available techniques. Further, even if the foreign network uses a less secure authentication mechanism, it still will not affect the EAP-CRA supplicants since their PMKs are supplied by the HOME AAA servers not-withstanding the limitations of the foreign network.

Another significant advantage of the EAP-CRA is its reliance on the HOME security credentials to secure its clients in the foreign network. Hence, it can be assured that the EAP-CRA clients will have the same security guarantee as in their home network in the foreign network. Further, in the case of EAP-TLS authentication with CA-signed PKI certificates, clients will need only a single set of certificates signed by the CA accepted by the HOME AAA server. There will be no need for clients to carry a number of different certificates to authenticate with different networks. Hence, in this context, the EAP-CRA facilitates EAP-TLS authentication and makes it more practical and viable.

Although there are many other techniques proposed for distributed authentication, the advantages of the EAP-CRA technique is its simplicity, robustness and versatility. Unlike many other systems that require additional components such as a token management system or federation of RADIUS servers, the EAP-CRA system depends only on the existing infrastructure, hence, assuring simplicity. The use of existing CA-signed PKI certificates without necessitating other authentication mechanisms such as tokens or smart cards enables the EAP-CRA system to be confined. Further, EAP-CRA system is not limited to WLAN or WiMAX, it can be effectively used with any wireless network, harnessing the unique security features of that particular wireless network. Furthermore, the authentication mechanism (EAP-TLS, EAP-TTLS, EAP-PEAP etc.) used by the wireless network does not influence the EAP-CRA system because it does use any form of mappings between these protocols and the EAP-CRA protocol.

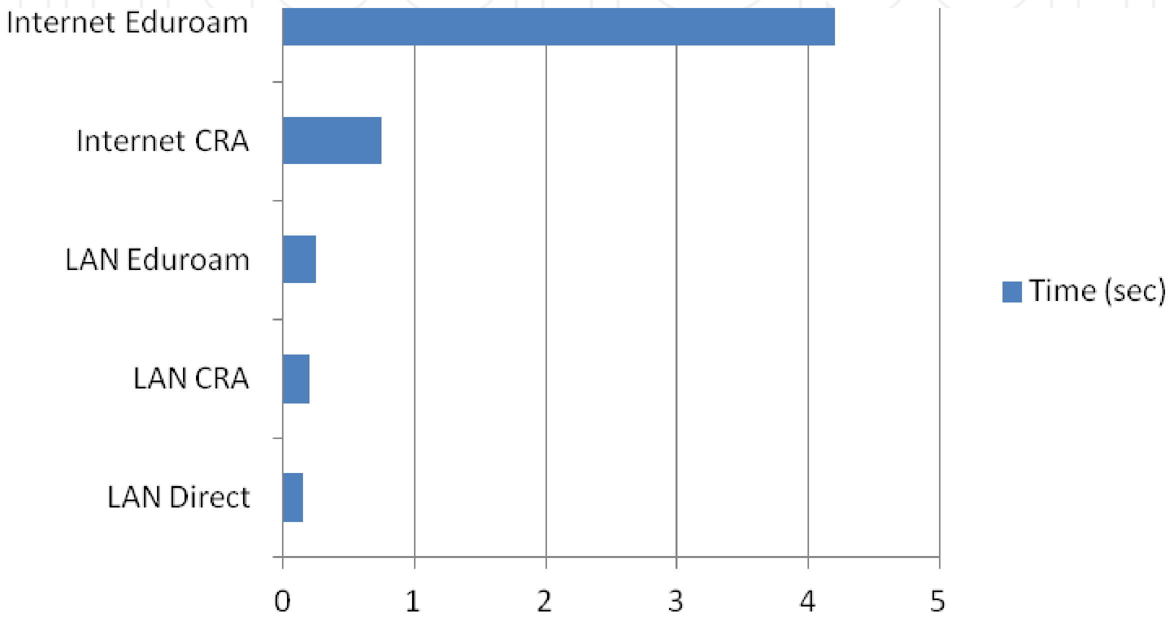

Figure 7. Comparison of Authentication Times

The above discussions illustrate the significance of the CRA approach and emphasize the need for a fast authentication mechanism as opposed to a hierarchical mechanism like the Edu-roam. Although Microsoft IAS provides a similar infrastructure to that of EAP-CRA, it is restricted to Microsoft EAP-PEAP authentications. In contrast EAP-CRA does not rely on any particular authentication protocol. It is designed to reap the maximum leverage of the authentication mechanism that is best for the particular home environment. Hence, when a hand-held device roams in a foreign network it will have the same security guarantee as in the home network.

EAP-CRA is differentiated by other EAP methods in the aspects of communication scope by covering both the foreign and the home authentication servers. Other EAP methods such as EAP-TLS or EAP-TTLS do not consider server to server communication. EAP-CRA provides authentication and communication privacy between the foreign and the home authentication servers based on public key infrastructure. The home and foreign servers have got the public certificates of each other. EAP-CRA encrypts the authentication message twice and then sends it to the other foreign server ensuring privacy and authenticity of the message. Any message from home server will first be signed by the home server’s private key and then by the foreign servers public key. Same process happens if the foreign server sends a message to the home server. The signature of a server by the private key authenticates the server to the other server and the public key encryption ensures privacy of the transmitted message. To implement the transmitting of the messages between two authentication servers EAP-CRA suggests using of RADIUS protocol by creating a new attribute field which encapsulates the EAP-CRA message. The EAP-CRA message is the double encrypted message which will be located in the value filed of the RADIUS attribute.

On the negative aspect, the effectiveness of EAP-ERP will depend on the mutual trust established between the participating AAA servers. If the AAA servers do not have any form of prior agreement, it will be up to the discretion of a FOREIGN AAA server whether to accept or deny an EAP-CRA request.

4. Enhancements to EAP-CRA

The Enhanced CRA protocol provides authentication in two modes; Full Authentication and Re-Authentication. With regard to mutual authentication CRA uses RADIUS servers as suggested in IEEE 802.1x. CRA suggests direct communication between radius servers by pre-arranged agreement or the servers could find each other dynamically. In case the RADIUS servers do not have a pre-arranged agreement they can use their CA-signed PKI certificates to ascertain trust between servers.

All AAA servers that participate in the CRA must possess a CA-signed PKI certificate and be capable of obtaining the CA-signed PKI certificates of other participating AAA servers. Assuming that all AAA Servers that participate in the CRA are in possession of their CA-signed PKI certificates, the CRA protocol can communicate between the FOREIGN and the HOME AAA servers securely.

4.1. Full EAP-CRA authentication

Initial assumption of the CRA protocol is that each mobile Node is primarily associated with a Network, which in this context is referred to as the Home network. The security of the Home network and the authentication mechanism used must be robust. It is assumed that an EAP method such as EAP-TLS, EAP-PEAP or EAP-TTLS is used in the Home network. Therefore the values for MSKName, MSK, EMSK and the Time To Live (TTL) for these keys are available for the Peer. Since some of the EAP methods utilize CA-signed PKI certificates to authenticate and secure the communication CRA extends it to add more flexibility to certificate based authentication. We have chosen WLAN as the medium to illustrate the components and messaging of EAP-CRA. Firstly, both the peer and the Foreign Access Point (FAP) discover their capabilities and decide on a suitable protocol to authenticate each other. If both parties are capable of EAP-CRA then the FAP will compose an EAP request message to solicit the identity of the Peer. It should be mentioned that the key for hashing function is generated from the EMSK.

In an unknown network, the peer will first check if the TTL of MSK is still valid. Expired MSK will lead to a failed authentication and will prompt a full authentication. The peer will be responsible to do a full authentication with its Home Network to obtain a fresh MSK. On the other hand, if the MSK is valid, the peer generates a random sequence number and encrypts the EMSKname of home network and the sequence number with the public Key of its HAS. The composed EAP-Response message will be sent to the FAP, which contains the encrypted message, Message Authentication Code, the realm of the home network and the random identity of the peer (message b in List 1).

List 1: Messages Exchanged During CRA Full Authentication

a. $FAP \rightarrow MN : EAP_{req}[ID]$Inline Formula

b. $MN \rightarrow FAP : EAP_{res}[Hostname,\ Realm_h, \{EMSKname,\ Seq\#\}UK_h, MAC]$ Inline Formula

c. $FAP \rightarrow FAS:\ ACC_{req}[Hostname, Realm_h, \{EMSKname,\ Seq\#\}UK_h,\ MAC]$ Inline Formula

d. $FAS \rightarrow HAS:\ ACC_{req}[Realm_f, \{Hostname\}PK_f, \{EMSKname,\ Seq\#\}UK_h]$ Inline Formula

e. $HAS \rightarrow FAS:\ ACC_{res}[\{Hostname\}PK_h,\ \{MSK_{CRA},\ EMSK_{CRA}\}UK_f, EAPsuccess,\ Seq\#]$ Inline Formula

f. $FAS \rightarrow FAP:\ ACC_{res}[MSK_{CRA},\ Realm_f, ReID, Seq\#, MAC]$ Inline Formula

g. $FAP \rightarrow MN:\ EAP_{req}[Realm_f, ReID, Seq\#, MAC]$ Inline Formula

h. $MN \rightarrow FAS : EAP_{res}[ACK, Seq\#, \mathrm{MAC}]$ Inline Formula

i. $FAS \rightarrow MN : EAP_{suc}$ Inline Formula

FAP will encapsulate this EAP-Response message inside a RADIUS Packet and forward it to the foreign authentication server. The FAS will also utilize RADIUS for server-to-server communication. However before sending the received message, the FAP will add its domain name and encrypt the MSKname with its Private Key (message d in List 1). This enables the HAS to authenticate the FAS. Upon receiving the message from a foreign network, HAS is able to check if the FAS is authorized based on the domain name of the FAS. The HAS can authenticate the FAS by verifying the contents of the signed message. Peer authentication will be managed by matching the MSKname with MSK, EMSK, Validation of key timer and the number of re-authentication of the peer. If the MSK is valid the HAS can combine the foreign domain name, sequence number and the previous EMSK to generate new CRA-MSK and CRA-EMSK.

After updating the timer and counter values of the MSKname the HAS creates a RADIUS message which holds Access Accept, encrypted values of CRA-MSK and CRA-EMSK with FAS's Public Key, MAC and privately signed message of domain name – MSKname (message e in List 1).

FAS first checks the signed MSKname to validate the HAS, then stores the MSKname and CRA keys. In addition to these it calculates a new timer, counter and random re-authentication ID for local re-authentication in case the peer stays for longer time in the foreign network. These values are CRA_timer, CRA_counter, and CRA_RND. The value of the CRA_timer must be less than the validity time of the initial MSK. Next, the FAS sends CRA_counter, re_id, EMSKname signed with HAS's private key, Foreign realm and CRA-MSK inside a RADIUS packet to FAP (message f in List 1). The CRA-MSK will be utilized for future communication to provide privacy. The rest of the message is sent to the peer (message g in List 1). The peer will be able to authenticate its home server by verifying the signature and can generate CRA-MSK and CRA-EMSK. It then creates a EAP-Response as an acknowledgment with MSKname. The FAS can then compose a EAP-Success message and send it back to the peer.

On receiving the EAP success message, the peer generates rMSK independently leading to the key distribution phase. The key distribution phase will be similar to that of the RSNA where the supplicant and the authenticator will use the MSK to derive the Temporal Session Key (TSK). Once the TSKs are derived normal data communication can commence.

4.2. EAP-CRA re-authentication

In the previous section we described a roaming-enabled authentication mechanism for users who wish to get connected to a new network, using the security credentials that they use in their home network. Although we anticipate relatively faster CRA authentication, in situations where the user continues to work on a foreign network the need for re-authentication is anticipated.

This section will explain the re-authentication process that can occur due to handover within the same network, i.e. when a user moves from one access point to another. The Enhanced CRA full authentication generates CRA-MSK and CRA-EMSK for a secure communication. Possession of these keys by the supplicant and the FAS can quicken the process of re-authentication. The FAS, after the successful authentication of a supplicant distributes the re-authentication identity and the CRA_Counter to the peer. The counter determines the number of re-authentications which can be acceptable.

The process of re-authentication will be initiated by the authenticator with EAP-Request for supplicant ID. In response the supplicant will check the time since last logon to verify the validity of CRA-MSK. In case the key is expired then a valid peer will fall back to request a full EAP-CRA authentication. On the other hand the supplicant sends its re-authentication ID and realm inside Kname-NAI, a random sequence number with a hashed value of the message. The key for the hash can be generated from the CRA-EMSK and sequence number. Here, the need for the sequence number arises to provide immunity against replay attacks. The authenticator will then forward the EAP-Response encapsulated as a RADIUS packet to the FAS (message c in List 2).

List 2: Messages Exchanged During CRA Re-Authentication

a. $FAP \rightarrow MN : EAP_{req}[ID]$ Inline Formula

b. $MN \rightarrow FAP : EAP_{res}[KeyNameNAI, Seq\#, MAC]$ Inline Formula

c. $FAP \rightarrow FAS : ACC_{req}[KeyNameNAI, Seq\#, MAC]$ Inline Formula

d. $FAS \rightarrow FAP : ACC_{res}[MSK_{CRA}, ReID, EAP_{succes}]$ Inline Formula

e. $FAP \rightarrow MN : EAP_{req}[ReID, Seq\#, MAC]$ Inline Formula

f. $MN \rightarrow FAS : EAP_{res}[ACK, Seq\#, MAC]$ Inline Formula

g. $FAS \rightarrow MN : EAP_{suc}$ Inline Formula

Upon receiving the message the FAS checks the Kname-NAI with its stored authentication information. If there is a match, the server generates the hash value to verify the validity of the message and update the CRA_counter and CRA_timer values. The FAS will then send MSK, MAC, SEQ number to the authenticator. The authenticator retains the MSK and sends the rest to the peer. In the final step, the peer sends an EAP-Response as an acknowledgment. At this point the client is able to calculate the keying material, however to start secure communication the peer waits until it received the EAP-success from the authenticator.

Two sequence numbers, one with HAS and other with FAS are maintained for replay protection of EAP-CRA messages. The sequence number maintained by the supplicant and HAS is initialized to zero on generation of EMSK. The server sets the expected sequence number to the received sequence number plus one on every successful Re-authentication request, i.e. on generation of DSRK. Similarly, the supplicant and the FAS maintain a sequence number with the generation of rMSK while the supplicant is in the FAS's domain.

4.3. Analysis

To substantiate the effectiveness our protocol we first examine the key security features of Enhanced CRA and then compare the cost involved in communication and computing between Enhanced EAP-CRA and its close competitor EAP-ERP.

4.3.1. Security consideration

RFC-3748 [17] indicates mandatory properties and security constraints of an EAP method such as freshness of session key and resistance against replay, dictionary and man in middle attacks. These features can be used as a reference to analyze the protocol in compliance with the EAP frame work. In this section we present our analysis of our protocol against this criterion.

Replay attacks: Generally replay attacks are initiated by re-using captured PDUs. The captured PDUs have authentic ingredients and can be replayed influencing legitimate nodes to respond. The CRA responds to this threat by the use of sequence numbers that enables both the sender and the receiver to have a record of the received datagram. If a packet is out of order it can be dropped. In case of re-authentication the sequence number is generated by the peer. For the rest of the session the peer and the foreign server will increment the value of this sequence number. In the process of full authentication the peer and HAS can benefit from the same procedure to protect against reply attacks.

Man In The Middle (MitM) attacks: In this category of attacks a rogue node introduces itself as a legitimate member in the communication. If there is no security mechanism in place the malicious node can continue to remain in between two legitimate nodes and subsequently masquerade as a legitimate node. During the EAP-CRA re-authentication process, MitM attacks are shunned with a Message Authentication Code (MAC). The MAC is simply a hash of the entire message that is attached to the original message. In this situation an attacker needs to have the knowledge of the hash key to revise the message and to re-calculate the hash. In case of full authentication, the use PKI certificate provides immunization against modification of messages.

Hiding User identification: The proposed method uses KeyName value as user's id during the full CRA process. This prevents from the real identity being revealed to an outsider. During the full authentication process, just before the EAP-Success message the FAS pass a re-authentication ID to the Peer in a secured message. Therefore when the peer requests for re-authentication there is a new random identifier for the peer.

Mutual Authentication:One of the essential features of every EAP method is mutual authentication. However, at the time of publishing EAP framework, the scope of EAP authentication was limited to peer-to-server authentication and the roaming attribute had not been considered. EAP-ERP may satisfy the condition of mutual authentication between Home server and the supplicant, but it is lacking of bilateral proof of identity between the supplicant and a foreign server. More importantly it relies on the security of RADIUS for server-to-server authentication. In contrast, EAP-CRA reaps the advantages of PKI to satisfy this need during the full authentication process.

As both EAP-CRA and EAP-ERP extend the scope of authentication process, the mutual authentication issue can be explored in three areas; between peer and home server, peer and foreign server, and the foreign and home servers. During full EAP-CRA authentication, the proof of possession of MSK (or a key generated from MSK) from the prior EAP authentication process validates the mutual identity between the peer and the home server. The mutual identity between the peer and the foreign server is realized by the foreign server generating a MAC from a key derived from the EMSK which both the foreign server and the peer are in possession. In return the peer also calculates a MAC value to place it inside the final message. This same model is valid for re-authentication phase as well.

Mutual authentication between servers is realized by each server using its private key to encrypt their hostnames. In this view, both servers sign the MSKname to authenticate each other.

4.4. Cost consideration

In this section we compare the cost of communication and computation between Enhanced EAP-CRA and EAP-ERP. It should be noted that EAP-ERP performs a full authentication with the home server every time it enters a foreign network. For this purpose we use EAP-TLS as the home authentication method.

EAP-CRA exchanges eight messages between the supplicant and the servers during full authentication. It also utilizes seven messages during the re-authentication process. In the case of ERP, a minimum of sixteen messages are exchanged between the supplicant and the servers.

This is made up of seven messages that are specific to ERP and at least nine messages from EAP-TLS, since we consider EAP-TLS as the home authentication method. For simplicity we are considering the size of the messages during these exchanges. Table 3 lists the number of messages used in each authentication methods.

When entering a foreign network, a station that uses EAP-ERP performs a full authentication with its home server. This process will be very time consuming due to the fact that all message exchanges should take place over the internet. This is a significant weakness of EAP-ERP compared to EAP-CRA for two reasons; 1) the number of messages and 2) the size of the messages. With regards to re-authentication, ERP re-authentication should take place much quicker as it uses only five messages. However, the actual time differences must be determined after the real setup of both protocols.

Authentication Method	No. of Messages
CRA Full Authentication	7
CRA Re Authentication	8
ERP Initial	16
ERP Re Authentication	5

Table 6. Communication Cost.

To evaluate the computational cost of the protocols we investigate the number of Hashing, Encryption and Decryption operations performed. Table 6 presents these values for EAP-CRA and EAP-ERP. In case of EAP-CRA full authentication there are four hashing operations and eight encryption operations. Initial EAP-ERP does not involve any encryption or decryption but it should be noticed that there will be at least 16 message exchanged while there are just 8 messages for full EAP-CRA authentication. Moreover the encryption involved in the process will ensure the security of the supplicant while it is roaming to a foreign network. In case of Re-authentication, cost of both protocols will be very similar as they both will perform four hash operations.

From the above comparisons we can say that EAP-ERP has high communication costs and Enhanced EAP-CRA has high computing costs. Therefore, we are expecting reasonable performance for Enhanced EAP-CRA due to the fact that communication overheads are normally more costly compared to the computational overheads.

	CRA Full-auth	CRARe-auth	ERPInitial	EAPRe-auth

Sup	Hash(2)
	Encrypt(1)
	Decrypt(1)
		Hash(2)
		Encrypt(0)
		Decrypt(0)
			Hash(0)
			Encrypt(0)
			Decrypt(0)
				Hash(2)
				Encrypt(0)
				Decrypt(0)

FS	Hash(2)
	Encrypt(1)
	Decrypt(1)
		Hash(2)
		Encrypt(0)
		Decrypt(0)
			Hash(0)
			Encrypt(0)
			Decrypt(0)
				Hash(2)
				Encrypt(0)
				Decrypt(0)

HS	Hash(0)
	Encrypt(2)
	Decrypt(2)
		Hash(0)
		Encrypt(0)
		Decrypt(0)
			Hash(0)
			Encrypt(0)
			Decrypt(0)
				Hash(0)
				Encrypt(0)
				Decrypt(0)

Table 7. Computational Cost

5. Conclusion

The main advantage of the CRA mechanism is the use of only two messages to authenticate a wireless device in a FOREIGN network. Although the time taken between the FAS and the HAS may vary depending on the traffic and/or capacity of the wired network, the use of only two messages in a FOREIGN network makes the CRA mechanism very much reliable compared to other available techniques. Further, even if the foreign network uses a less secure authentication mechanism, it still will not affect the CRA clients since their MSKs are supplied by the HASs not-withstanding the limitations of the foreign network.

Another significant advantage of the CRA is its reliance on the HOME security credentials to secure its clients in the foreign network. Hence, it can be assured that the CRA clients will have the same security guarantee as in their home network in a foreign network. Further, in the case of EAP-TLS authentication with CA-signed PKI certificates, clients will need only one certificate signed by the CA and accepted by the HAS. There will be no need for clients to carry a number of different certificates to authenticate with different networks. Hence, in this context, the CRA facilitates EAP-TLS authentication and makes it more practical and viable.

Although there are many other techniques proposed for coordinated authentication, the triumph of the CRA technique is its simplicity, robustness and versatility. Unlike many other systems that require additional components such as a token management system or the Kerberos servers, the CRA depends only on the existing infrastructure, hence, assuring simplicity. The use of existing CA-signed PKI certificates without necessitating other authentication mechanisms such as tokens or smart cards enables the CRA mechanism to be confined. Further, the CRA mechanism is not limited to WLAN, WiMAX or 4G LTE, it can be effectively used with any wireless network, harnessing the unique security features of that particular wireless network. Furthermore, the authentication mechanism (EAP-TLS, EAP-TTLS, EAP-PEAP etc.) used by the wireless network does not influence the CRA mechanism because it does use any form of mappings between these protocols.

On the negative aspect, the effectiveness of the CRA mechanism will depend on the mutual trust established between the participating AAA servers. If the AAA servers do not have any form of prior agreement, it will be up to the discretion of FAS whether to accept or deny a CRA request.

Author details

E. Sithirasenan, K. Ramezani, S. Kumar and V. Muthukkumarasamy

School of Information and Communication Technology Griffith University, Gold Coast, Australia

References

[1] IEEE StdWireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", (1999).

[2] IEEE Std(2004). IEEE Standard for Local and metropolitan area networks: Part 19: Air Interface for Fixed broadband wireless access systems., 16-2004.

[3] Ghosh, A, Ratasuk, R, Mondal, B, Mangalvedhe, B. N, & Thomas, N. T. LTE-advanced: next-generation wireless broadband technology", in *IEEE Wireless Communications*, Aug. (2010). , 17(3), 10-12.

[4] He, C, & Mitchell, J. C. Security Analysis and Improvements for IEEE 802.11i", in *Proceedings of the 12th Annual Network and Distributed System Security Symposium*, NDSS (2005). , 90-110.

[5] Perrig, A, Stankovic, J, & Wagner, D. Security in wireless sensor networks", Wireless Personal Communications, (2006). , 37(3-4)

[6] IEEE Standard 802i Part 11, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 6: Wireless Medium Access Control (MAC) Security Enhancements," July (2004).

[7] Lynn, M, & Baird, R. Advanced 802.11 attack, Black Hat Briefings, July (2002).

[8] Asokan, N, Niemi, V, & Nyberg, K. Man-in-the-Middle in tunneled authentication protocols. Technical Report (2002). IACR ePrint archive, United Kingdom, Cotober 2002.

[9] IEEE Std 802X-2001, "Local and Metropolitan Area Networks- Port-Based Network Access Control", June (2001).

[10] Iyer, A. P, & Iyer, J. Handling mobility across WiFi and WiMAX", in *Proceedings of the 2009 international Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, IWCMC (2009). , 537-541.

[11] Machiraju, S, Chen, H, & Bolot, J. Distributed authentication for low-cost wireless networks", in *Proceedings of the 9th Workshop on Mobile Computing Systems and Applications*, HotMobile (2008). , 55-59.

[12] Almus, H, Brose, E, Rebensburg, K, & Kerberos-based, A. EAP method for re-authentication with integrated support for fast handover and IP mobility in wireless LANs", in *Proceedings of the 2nd international conference on communications and electronics,* ICCE (2008). , 61-66.

[13] Huang, Y. L, Lu, P. H, Tygar, J. D, & Joseph, A. D. OSNP: Secure Wireless Authentication Protocol using one-time key", in *Proceedings of Computer and Security* (2009). , 803-815.

[14] Narayanan, V, & Dondeti, L. EAP Extensions for EAP Re- authentication Protocol (ERP)," RFC 5296, Internet Eng. Task Force, (2008).

[15] Salowey, J, Dondeti, L, Narayanan, V, & Nakhjiri, M. Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)," RFC 5295, Internet Eng. Task Force, (2008).

[16] Sithirasenan, E, Kumar, S, Ramezani, K, & Muthukkumarasamy, V. An EAP Framework For Unified Authentication in Wireless Networks". In TrustCom'11: *Proceedings of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, Nov. (2011). , 92-99.

[17] Blunk, L, & Vollbrecht, J. PPP Extensible Authentication Protocol (EAP)," RFC 3748, Internet Eng. Task Force, (2004).

[18] Stanke, M, & Sikic, M. (2008). *Comparison of the RADIUS and Diameter protocols.* Paper presented at the Information Technology Interfaces, 2008. ITI 2008. 30th International Conference.

[19] Aboba, B, & Simon, D. PPP EAP TLS Authentication Protocol," http://tools.ietf.orgwg/pppext/draft-ietf-pppext-eaptls/draftietf-pppext-eaptls-06.txt, August (1999).