The 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'07)

FAST RE-AUTHENTICATION PROTOCOL FOR INTER-DOMAIN ROAMING

Maryna Komarova Michel Riguidel Artur Hecker
ENST
46 rue Barrault, Paris 13, France

ABSTRACT

In this paper we introduce the Fast re-Authentication protocol (FAP) for inter-domain roaming, which aims to reduce authentication delay of a mobile user in a visited administrative domain. The approach eliminates the need of communication between the target and the user's home networks for credentials verification and uses a short-living lightweight re-authentication ticket that does not require revocation mechanism. The proposed approach does not depend on the nature of roaming agreements between different networks.

I. INTRODUCTION

The use of wireless networks in a public sphere claims for a higher level of security based on strict network access control and communication data encryption. These requirements have been satisfied in the 802.1X standard [1], which implements the Extensible Authentication Protocol (EAP) [2]. EAP supports different authentication methods that provide mutual authentication, are transparent for a user and create material for encryption keys derivation at both the network and the client side.

The overlapping of different network operators' coverage areas permits users to choose at any time an access network with more appropriate characteristics (bandwidth, service cost etc.). The user terminal (UT) may execute a handover between the points of attachment either within the same administrative domain or in domains managed by different authorities. In this local scope the changing of network should not have a negative effect on a session running at the user's terminal.

The existent models and protocols for authentication are not efficient for inter-domain mobility. This work specifies an EAP mechanism for a fast authentication in the inter-domain handover. The Fast re-Authentication Protocol is technology independent and may be implemented over any wireless network (e.g., 802.11, 802.16 or 3GPP supporting EAP). For illustration purposes we here use IEEE 802.11.

The proposed protocol consists of two sub-protocols: the ticket acquisition and the fast re-authentication. The former is executed after the user is attached to the network and requires inter-domain communication. This phase is not critical in term of the handover performance. The latter is executed during the handover and localizes the authentication process in the target domain. FAP uses symmetric cryptography and avoids sophisticated schemes for user-related data management.

This paper is organized as follows. Section 2 introduces the background, Section 3 describes the proposed Fast re-Authentication Protocol in detail, and Section 4 shows simulation results for the proposed method. In Section 5 we analyze the developed protocol and Section 6 concludes the paper.

II. BACKGROUND

The authentication has a significant impact on the handover latency. To allow a normal execution of a Voice over IP application on the UT, the maximum handover duration must not be more then 150 ms according to [3], while our experiments and [4,5] have shown a latency more than 300 ms just for 802.1X authentication using EAP-TLS method.

EAP methods were designed without taking into consideration inter-domain roaming and application session continuity support. There are two fundamental approaches for authentication between the user terminal and the visited network. The first one requires communication between the visited and the home networks during the authentication process to verify user's credentials. These communications cause delays difficult to predict and to shorten. The second group of approaches is based on public key cryptography. Using X.509 certificates [6] may eliminate the necessity of the inter-domain communication during the authentication process, but in this case authentication is only possible if both the UT and the visited network recognize each other's certification authorities. Disadvantages of the method are a heavy computational cost of asymmetric cryptography operations and a need for a certificate revocation mechanism.

For IEEE 802.11i, fast authentication methods that modify the standard [7, 8] have shown good results for intra-domain handovers and represent an attractive perspective to use them for inter-domain roaming. But such extensions of proposed approaches require establishment of trust relationships between internal entities of different networks, such as access points or access routers. Using access routers as authenticators makes the authentication technology-independent, but opens access to the network at the link-layer for all potential clients.

III. PROPOSED AUTHENTICATION APPROACH

The proposed method is based on symmetric cryptography and uses a challenge-response mechanism. The access to the target network is granted to the user if the latter proves that he was recently successfully authenticated by a roaming partner of the target network. This proof is contained in the ticket given to the user by the roaming partner. In the encrypted part the ticket contains information known by the user and only the issuer and the addressee can decrypt this information. In such a way the user is able to check the identity of the target network. FAP also establishes key material between the two authenticated parties.

A. Assumptions

Fast re-Authentication Protocol (FAP) specifies communication between the FAP Server (FAPS) at the network side and the FAP Client (FAPC) at the UT. The

mobile user can roam from one non-home network to another. To distinguish these visited networks we will call the one where the user has been authenticated the *current network* and that which the user is roaming to the *target network*. We also assume that there are roaming agreements either between the home and the target networks or between the current and the target networks. Authorities that have roaming agreements share symmetric or asymmetric keys $\boldsymbol{K}$= $\{\boldsymbol{K_R}\}$. The user can communicate in a secure manner with his home domain. The operation of the proposed protocol does not depend on the nature of the security associations between partner domains (they may use either symmetric or asymmetric cryptography).

The operation of FAP is based on the assumption, that the UT is attached to a network and has performed an initial full authentication by some other means.

In the FAP model, both the current network of attachment and the home network may generate tickets for a client. We call the entity that is able to create tickets for a particular user the anchor FAPS and, to simplify an explanation, denote it as FAPS.

B. Ticket acquisition phase

Ticket acquisition protocol provides a user with credentials for a further fast authentication. Upon a request sent by the FAPC, the FAPS generates tickets and does not care about ticket renewing and revocation. If the ticket expires, the new one is generated exclusively upon the user's request.

1) Ticket generation by the user's home network

If a UT is attached to its home network, it is authenticated by this network. Otherwise, being attached to a visited network, it may communicate with its home network for the reason of, for example, authentication or location update.

Whatever the case, the UT and its home network share some secret information. After a successful authentication, both entities keep data that depends on the used method and may be, for example, a Master Secret for 802.11X authentication.

2) Ticket generation by the current network

If the UT is originally attached to the visited network, it performed a previous successful authentication in this network and both the user and the network have generated key material as mentioned in Section III.B.1.

On the user's request the visited network creates tickets only for its neighbors. The current network has a responsibility to decide whether tickets for its partners must be sent to the authenticated client.

3) Authentication ticket format

The idea of the method is to use a short-living lightweight ticket, which does not require any revocation mechanism and may be verified only by the issuer and the target network. The ticket format is presented in Figure 1.

The ticket is bound to the issuing and the target networks by the usage of the key $\boldsymbol{K_R}$ shared between the two domains. It is also bound to the user by the user pseudonym and the previous authentication result, which are described further.

C: part in-clear	
target_name	72 bytes
issuer_name	72 bytes
expires	6 bytes
S: encrypted part {	
auth_res	32 bytes
user_pseudonym	72 bytes
}K_R	
	254 bytes
Signature SHA-256(C|S, K_R)	***32 bytes***

Figure 1: Ticket format

The ticket consists of two parts. The section S (further called secret) is encrypted with the key $\boldsymbol{K_R}$ shared with a particular roaming partner of the ticket issuer. The authentication result "*auth_res*" is produced from information related to the previous authentication as shown in (2). As the target FAPS (tFAPS) must obtain the user name [9], the latter is presented in the ticket. On the other hand, the identity of the user should be hidden. To satisfy this requirement the "*user_pseudonym*" is a roaming pseudonym of the user. This pseudonym is the user identity perceived by the non-home network in the initial authentication. It is not equivalent to the username in a general case.

The part C (see Figure 1) is not encrypted. It contains "*target_name*" that is the name of the destination network, "*issuer_name*" that is the name of the network, which have provided the ticket and the "*expires*" field, which determines the end of the ticket validity period. This ticket expires after a short period of time (defined by the issuer).

The "*target_name*" represents the identity name of the partner of FAPS. As one authority can manage several networks (i.e., UMTS and WiFi hotspots) its name presentation may vary on different interfaces. To make the ticket format technology independent and to avoid generation of more than one ticket per roaming partner, the FAPS provides the FAPC with a function matching different seen names of a network to the "*target_name*":

$$seen\_name \rightarrow target\_name \quad (1)$$

The cFAPS knows which "*seen_name*" are visible from it and sends to the FAPC the correspondence between these names and the "*target_name*" contained in the ticket. The FAPC may hold permanently the function provided by its home FAPS, and the latter does not care about the nature of the current neighborhood of the subscriber.

The entire ticket is signed with the key $\boldsymbol{K_R}$ to assure its integrity protection. For ticket encryption and signature the FAPS may use either a single key or separate keys against the security association between the partner networks.

4) Ticket acquisition procedure

Figure 2 illustrates the flow chart of ticket acquisition. When the user terminal is attached to a network, we assume that a strong mutual authentication is completed between them (it may either be an initial authentication or a re-authentication after FAP accomplishment). In this situation the user terminal trusts its home domain via some shared data and the current domain via the authentication result. The user terminal sends a **Ticket request** message to the home network and to the current network, if the latter has indicated

during the authentication phase that it supports ticket distribution.

After an initial authentication, UT and the network (typically an authentication server) share fresh key material derived in the authentication phase. We call this material *method_res* in a generalized manner. The network, trusted by the user, creates an authentication ticket that contains the result of the previous authentication *auth_res*.

The *auth_res* is derived from the *method_res* both by the anchor FAPS and by the FAPC as (2) shows. "||" denotes concatenation. The pseudo-random function (PRF) is calculated according to [10].

$$auth\_res = PRF(method\_res, user\_pseudonym \,||\, cMAC) \quad (2)$$

We presume that the FAPS encrypts the secret part of the ticket with a key $\boldsymbol{K_R}$, shared with a particular roaming partner. It completes the ticket with the date and the time of ticket expiration, target network name and its own name. Finally the FAPS signs the entire ticket with the key $\boldsymbol{K_R}$ and sends it to the FAPC upon the Ticket Request. The FAPC is not able to decrypt the secret part of the received ticket.

Each authentication server keeps a list of roaming partners and a list of subscribers that change only when a subscriber or a roaming partner is added or eliminated.

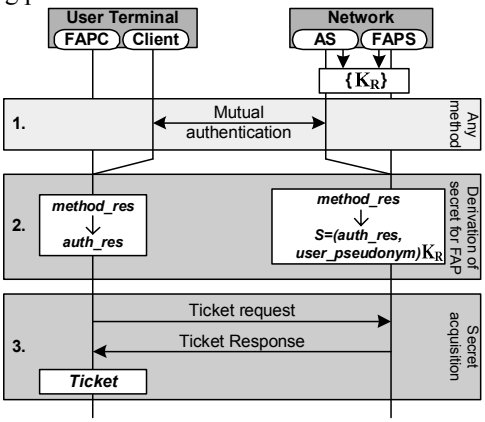

Figure 2: Ticket acquisition flow chart

We assume that they share keys and may communicate in a secure manner. The FAPC sends **Ticket request** to the FAPS (see Figure 2) and signs it with a key shared between them. After verification of the received request the FAPS answers with **Ticket Response** message. This message is encrypted and signed with the key shared with the FAPC.

C. Inter-domain handover authentication

FAP provides authentication of the client and the visited network without any communication between the target and the user's home network and enables secure negotiation of a shared secret between the UT and the target network.

The client has an encrypted and signed ticket, which the tFAPS can verify. To decrypt and verify the ticket the target server (tFAPS) uses a key from the security association with the issuer of the ticket. Figure 3 shows the information flow in the authentication exchange.

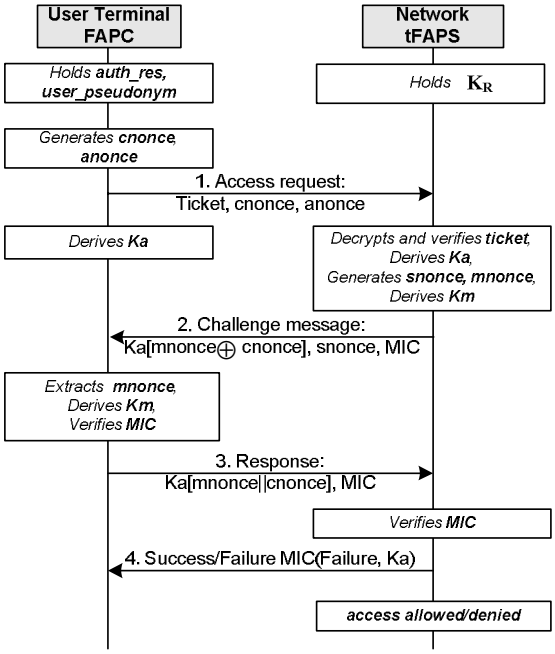

Figure 3: Flow chart of the FAP authentication exchange.

1) Cryptographic functions

cnonce and *anonce* are random numbers generated by the FAPC. *snonce* and *mnonce* are random numbers generated by the FAPS.

$\boldsymbol{K_a}$ is the authentication key, which is derived from the data contained in the ticket *auth_res*, the random number *anonce*, the address of the UT's network interface *cAddr* and the *user_pseudonym* as shown in (3). This PRF is calculated according to the algorithm described in [10]. The protocol uses block-cipher encryption.

$$K_a = PRF(auth\_res, "authentication \quad key", anonce \,||\, cAddr \,||\, user\_pseudonym) \quad (3)$$

$\boldsymbol{K_m}$ is the Master Secret, which is generated in case of successful authentication and serves as a material to session keys derivation. This key is calculated as follows:

$$K_m = PRF(auth\_res, "master \quad secret", \min(cnonce, mnonce) \,||\, \max(cnonce, mnonce) \,||\, user\_pseudonym) \quad (4)$$

The *MIC* denotes Message Integrity Code; it is computed over the body of the message (denoted as *msg*) using the Master Secret $\boldsymbol{K_m}$ as shown in (5).

$$MIC = HMAC - SHA - 256(K_m, msg) \quad (5)$$

2) Message exchange

The FAPC sends **Access Request** message to start authentication process with the tFAPS. This message contains user credentials and provides the tFAPS with the material for further key generation. After sending the ticket, the FAPC calculates an authentication key $\boldsymbol{K_a}$. On reception of

message 1 the tFAPS searches in its database of roaming partners a key shared with the domain, correspondent to the "*issuer_name*". If the domain name is found, it decrypts the ticket with a correspondent key K_R and calculates K_a in the same way as the client. The tFAPS generates a random value *snonce* and derives a Master secret K_m, as shown in (4).

The tFAPS cancels authentication and responds with a **Failure message** if the mentioned authority is unknown, if tFAPS cannot decrypt the ticket or if the ticket has expired.

The tFAPS replies with **Challenge message** (message 2) to the FAPC. This message contains the result of XOR function of *cnonce* and *mnonce*, encrypted with K_a, the *snonce* and the integrity code of the entire message, computed using K_m according to (5). Sending this message, the tFAPS proves that it corresponds to the authority mentioned in the ticket. On reception of this message the FAPC extracts the *mnonce*, derives K_m in the same way as the tFAPS and verifies the message integrity code. If the computed and received values of MIC do not match, verification fails. That is possible if K_a is not derived correctly, if *cnonce*, used by the tFAPS, is not valid or K_m is not derived correctly. In this case the FAPC silently discards the received message. FAPC knows K_a, and *cnonce*, thus it is able to extract *mnonce*. The value of *snonce* is not encrypted, so the client can derive K_m and calculate MIC. It compares the calculated MIC with the received MIC.

If the verification was successful, the FAPC sends **Response message** to the tFAPS. This message demonstrates to the tFAPS that the client is the same that has started the exchange and allows the tFAPS to verify if the FAPC has derived the same Master secret K_m. The presence of *mnonce* encrypted with K_a serves to prevent Man-in-the-Middle attack. The tFAPS responds with **Success message**, if the calculated MIC matches the MIC included in the Response message. Otherwise the tFAPS sends **Failure message** to the FAPC.

The Master secret K_m may be used for further generation of session keys.

If the target network does not support FAP, the UT should perform a full authentication using a standard method supported by the network.

IV. Performance Evaluation

This section provides the evaluation of average re-authentication latency and the load of authentication servers for the proposed Fast re-Authentication Protocol.

A. Description of the Simulation Model

We have modeled the protocol operation on a small area covered by four public access networks, which have symmetric roaming agreements. The used number of mobile networks is sufficient for illustration of all considered situations of the presence of roaming agreements between network operators. In our model, two networks have roaming agreements with all neighbors and two networks have only one partner among its neighbors. In these conditions mobile clients are obliged to solicit tickets both to the home and the current networks. Each user can execute many inter-domain handovers during a session. Each network keeps databases of its roaming partners and its subscribers. The aim of the simulation was to estimate the authentication latency of the FAP and to compare it with a standard protocol. As an example of the latter we have taken EAP-TTLS with MD5 authentication.

To analyze the protocol performance, a model was created using OmNet++. For the first step the cryptographic primitives were implemented on a computer platform with a Pentium(R) 4 CPU (1.50GHz). Parameters used in the simulation model are shown in Table 1.

Table 1: Simulation Parameters

Operation	Value
PRF calculation	4.42368 ms
SHA-256 signature	0.03456 ms
AES encryption	0.00321 ms
propagation delay	1-2 ms

Experiments were held with three types of user mobility: low mobility, corresponding to a user walking at a speed of about 4km/h, medium mobility - 11km/h and high mobility – 40 km/h for a city bus. Each experiment lasted 14 simulated hours. We have studied the impact of following parameters on the performance of the protocol: user mobility and a number of users in the environment.

B. Simulation results

We have compared the simulated authentication time for FAP and EAP-TTLS with MD5. The aim of the simulation was to show the difference between the performance of the proposed and implemented mechanisms but not the exact authentication latency that depends on the platform and the implementation. The average estimated authentication latency was *13.60 ms* for FAP and *51.32 ms* for EAP-TTLS with MD5. Thus, the proposed protocol significantly reduces the authentication delay.

Our experiments have shown that the input and output data rate at the FAPS side growth linearly with the increasing number of users in the studied region. As the output data rate is proportional to the number of tickets sent, it is important to reduce the number of secrets sent to a user.

V. Analysis of the Protocol

A. Security Considerations

The operation of FAP is based on the result of the previous successful strong mutual authentication between the user and a network and does not depend on the used method. The protocol is supposed to be used only for user re-authentications during inter-domain roaming.

The proposed authentication protocol corresponds to requirements formulated in the RFC 4017 [9] to ensure protection of the user, the home and the visited network. Below we provide an analysis of security threats. Due to the nature of wireless network all traffic is visible for a potential attacker.

Ticket interception. During the ticket acquisition phase an attacker may steal a ticket. The interceptor cannot

impersonate the valid user with the ticket at the authentication phase because he is not able to decrypt the secret part and does not have enough information to reply to the Challenge message sent by the tFAPS.

Impersonation. The user cannot authenticate a fake network unless the latter has decrypted the ticket. The exchange of Challenge and Response messages in the authentication phase serves for protection against the Man-in-the-Middle attack.

To impersonate the valid user the attacker must have full access to the information kept on the user terminal.

Modification of information. We assume that the user and its home network share some secret and the anchor network signs the Ticket Response message during the ticket acquisition phase. So the user is able to detect data modifications. During the authentication phase the target network can verify the signature of the ticket and, if it is not valid, the tFAPS does not continue authentication.

Discovery of keys. The third party that has revealed the authentication key or a key derived from the key material cannot guess the information used for their generation because all keys are calculated using one-way pseudo-random function. The keys are mutually generated and are not transmitted between the FAPC and the FAPS.

Denial of service attack. At the end of the authentication phase, the malicious node cannot realize DoS attack as the Failure message is signed with $\boldsymbol{K_a}$ and the FAPC can authenticate its origin.

Service stealing attack. If the FAPS is compromised or one of the roaming shared keys is exposed then tickets can be created on its behavior. To privilege its own subscribers and to prevent denial-of-service attacks a network may limit the number of users that can be served in a time period (e.g. per day or per hour) par partner.

B. Related Work

H. Wang and A. R. Prasad in [11] introduce the idea that the current network can play a role of the trusted third party in the authentication of a mobile user to a target visited network. Authentication solutions proposed in [12] and [13] modify classical PKI in order to reduce certificate processing time and avoid problems related to certification authority interactions. The approach proposed in [12] is suited for the federation of networks with multilateral roaming agreements but it is difficult to implement in case of bilateral trust. The Localized Authentication [13] requires heavy management of credentials, and its public key cryptography operations cause high authentication latency.

The proposed Fast re-Authentication Protocol also implements the concept of recommendation credentials but it differs from approaches described above in some points. As the authentication ticket may be created both by the home and by the current network the approach extends the mobility region for the mobile user. The proposed authentication ticket does not require any management due to its short validity period. We propose a user terminal-driven authentication scenario, which eliminates communication between different networks.

VI. Conclusions and Future Work

In this paper we have presented Fast re-authentication Protocol for inter-domain roaming. FAP localizes the authentication process, eliminates the need for heavy management of user credentials and minimizes communication between different domains. The aim of the proposed solution is to minimize the authentication time and, consequently, the overall time of inter-domain handover. In-session inter-domain communication is steel needed for management and ticket acquisition reasons. However, these interactions are not critical for a handover process.

FAP allows mutual generation of key material, which serves to produce session encryption keys.

The protocol is supposed to be implemented for the first authentication in a new target administrative domain. All subsequent authentications within the same domain may be optimized using intra-domain fast re-authentication methods such as described in [5, 6].

The knowledge of the neighborhood of the current network of attachment of the client may be used to reduce the number of tickets generated and sent to each user. If the FAPS knows the current location of its subscriber and it knows, which partners adjoin with its network, it only generates and sends tickets for these partners.

Our future work addresses an optimization of the ticket distribution and implementation of the FAP.

References

[1] IEEE, Standards for local and metropolitan area networks: Standard for port based network access control, IEEE Standard P802.1X, October 2001

[2] B. Aboba et al., "Extensible Authentication Protocol (EAP)", Request for Comments 3748, June 2004

[3] International Telecommunication Union, "Transmission performance objectives and Recommendations", ITU-TG.102, 1990

[4] B. Aboba, Fast Handoff Issues (IEEE 802.11i draft, work in progress)

[5] I. Martinovic, F. A. Zdarsky, A. Bachorek, and J. B. Schmitt, "Measurement and Analysis of Handover Latencies in IEEE 802.11i Secured Networks", in Proc. of European Wireless 2007, Paris, France, April 2007

[6] R. Housley, W. Ford, W. Polk and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", Request for Comments 2459, April 2002

[7] IEEE, Standards for local and metropolitan area networks: Amendment 6: Medium Access Control (MAC) Security Enhancements, IEEE Standard 802.11i, July 2004

[8] M. S. Bargh et al, "Fast authentication Methods for handovers between IEEE 802.11 Wireless LANs", WMASH'04, October 1, 2004

[9] D. Stanley, J. Walker and B. Aboba, "Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs", Request for Comments 4017, March 2005

[10] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[11] H. Wang, A. R. Prasad, "Fast Authentication for Inter-domain Handover", in Proc. of International Conference on Telecommunications (ICT'04), Fortaleza, Brazil, August 1-7, 2004.

[12] Z. Hong, H. Rui, Y. Man, K. Zhigang, Q. Hualin, "A Novel Fast Authentication Method for Mobile Network Access", International Conference for Young Computer Scientists, Harbin, October, 2003

[13] M. Long, Ch.-H. "John" Wu, J. D. Irwin, "Localized Authentication for Wireless LAN Inter-network Roaming", Communications, IEEE Proceedings-Volume 151, Issue 5, 24 Oct. 2004 Page(s):496 – 500