Real-Time Inter-domain Handover Re-authentication Protocol

Radu Lupu[1], Eugen Borcoci[1], Dan Galatchi[1], and Tinku Rasheed[2]

[1] University Politehnica of Bucharest, Bucharest, Romania
[2] CREATE-NET, via alla cascata 56D. Povo, 38123 Italy
{rlupu,eborcoci,dgalatchi}@elcom.pub.ro,
tinku.rasheed@create-net.org

Abstract. Several statistics achieved to date on the Internet attacks have shown that one of the major causes for their proliferation is the scarce deployment of entity authentication mechanisms. Providing seamless support for real-time applications during the inter-domain handover procedure is one of the issues that still hinder the adoption of the network entity authentication service. In this paper, we focus on the design of a novel handover re-authentication protocol that can allow overcoming the current state. Furthermore, we also define the overall requirements for the underlying class of cryptographic methods which shall be used to implement our protocol. Thereafter, we present the preliminary results that were achieved on the re-authentication protocol validation.

Keywords: Authentication, real-time handover, wireless networks.

1 Introduction

The definition and integration of the security measures within the communication network infrastructure from its early stages of design represents a important task and challenge in recent times. In this paper, we focus on the design of the terminal handover re-authentication service for hybrid wireless mesh networks (composed of WiFi and WiMAX interfaces) [1]. In recent times, considerable research work has been performed or still in progress, in the field of handover re-authentication protocols and architectures, with notable results [4],[5],[7],[11],[12],[21],[23]. But, the inter-domain re-authentication of entities with support for real-time applications is still an open issue. Most of the re-authentication solutions proposed implied at least one transaction with the home domain (over Internet) during the handover process [6], which in turn increased significantly their latency (hundreds of milliseconds) and make them to be improper for real-time applications. Empirically, it has been shown in this case, that 90% of the latency is due the communication over Internet with the home domain [6]. Consequently, several proactive and reactive techniques were researched in order to avoid communication with the home domain during the handover process. However, all of these solutions experience some major drawbacks, such as: increased number of trust relationships required and domino effects [5],[11],

I. Tomkos et al. (Eds.): BROADNETS 2010, LNICST 66, pp. 473–482, 2012.

increased processing power due the use of asymmetric cryptographic mechanisms, or require seamless public-key infrastructures deployments [21].

We claim that our solution can overcome these limitations due a different approach which relies on the use of the re-authentication key derivation method with some special cryptographic properties. The main properties of our re-authentication protocol are:

- minimal inter-domain re-authentication latency (comparable with a local authentication) due to the re-authentication key (AK) derivation method;
- robustness with respect to the connectivity issues of the communication path in between visiting and home domains, through delegation of the re-authentication server role from home domain to the visiting domain. The connectivity issues are considered a common event within the networks with dynamic topology;
- low communication complexity through the use of the identity-based mechanisms;
- lower processing complexity through the use of symmetric techniques for more frequent events (e.g. within re-authentication mechanism), and asymmetric techniques for less frequent events (e.g. whenever a new re-authentication key is derived). It is expected, this property will enable the protocol to be run even on the mobile nodes with modest resources;
- completely avoids the costs entailed by the public-key certificates infrastructure management;
- minimize number of trust relationships involved by the re-authentication procedure (for instance, no trust relationships are required in between the current domain and its neighbors);
- prevents the domino effect, whenever one of the security architecture components is compromised.

The paper is organized as follows: Section II discusses the overall security architecture including a definition of the main functional components and their interactions in order to achieve the (re-) authentication services required. The proposed re-authentication protocol is specified in Section III. Thereafter, key derivation method design requirements and properties are outlined. Furthermore, we shortly describe how the re-authentication key material shall be managed. Section IV defines the validation process that we carried out on the re-authentication protocol to prove its security properties. This paper ends with Section V that concludes on the current status of the work and points out the future works.

2 The Security Architecture

In this section, we depict the security architecture for which our authentication protocol was initially designed. This security architecture was proposed as solution for implementation of the entity authentication, authorization and access control functionalities for the hybrid wireless mesh access network developed within the SMART-Net project [1]. According to the overall SMART-Net business model and network architecture, the security architecture design fits the two separate security administration domains corresponding to the RANP (Radio Access Network Provider) and BANP (Backhaul Access Network Provider) access networks, as defined in [1]. Due to the similarity of the RAN (Radio Access Network) and BAN (Backhaul Access Network) network functionalities, the security architecture design for RAN is analogous to the one for BAN (see Figure 1). Our security architecture design relies on the underlying 802.1x model (see [25]) due its extensibility and flexibility properties. These properties provide our solution the capabilities required to operate on hybrid and dynamic L2 network environments.

More specifically, our solution can work over either 802.11 or 802.16 infrastructures; and it allows partial auto-reconfiguration of the stakeholders' role (supplicant-authenticator) according to the network infrastructure modifications and allows security parameters negotiation (e.g. cryptographic algorithms). Most of these properties are due the integration of the EAP protocol within the 802.1x security model. Moreover, this model facilitates the local centralization of the management of the entities' credentials.

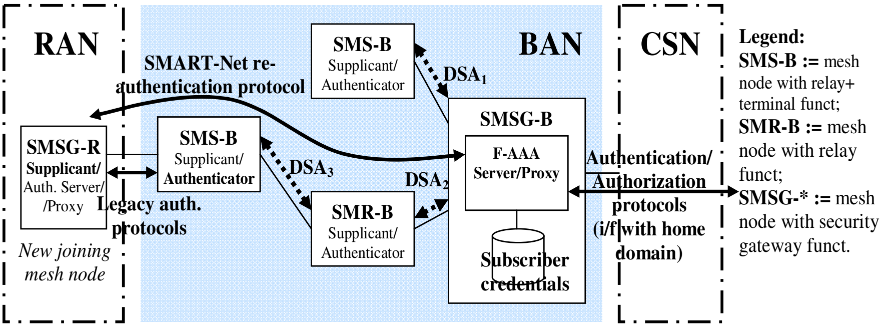

Fig. 1. The overall BAN's security architecture

In the following, we point out the main BAN's security architecture components and their roles:

- All wireless mesh nodes (e.g. SMS-B, SMR-B as shown in Figure 1) shall be capable to play supplicant, as well as, authenticator role in order to allow incremental buildup of the secure hybrid mesh infrastructure, while network entities are joining/leaving the infrastructure;
- One amongst the BAN mesh nodes has been assigned the security gateway role (denoted here SMSG-B). It is in charge with the BAN's security policy enforcement and control. SMSG-B can play either the role of a backend (re-) authentication and authorization server (F-AAA module) for subscribers /authenticated terminals, or the proxy role for authentication and authorization of the visiting network entities that enter the network for the first time. The mobile network entities shall be a priori registered and theirs credentials stored in a database that is accessible to the security gateway. For the case of real-time inter-domain handover, the SMSG-B should have the required functionality to allow efficient re-authentication procedures to be run locally, as much as possible.

Also, the SMSG-B entity is responsible for obtaining authorized connectivity service from the upstream network, on behalf of all mesh nodes within its RAN/BAN;

- Both dynamic (DSA) and static (SSA) security associations will be used to implement cryptographic-based security services. For enabling authentication service, it is assumed that each entity SMS-B or SMSG-B shares a pre-established SSA with the corresponding backend authentication server placed within the home domain. This SA is defined at the time of device (i.e. SMS-R/B, SMR-R/B or SMSG-R/B) registration to some domain. In addition, SSAs are pre-established in between SMSG-B (AAA modules) from several BAN domains, to ensure AAA's protocol security. DSAs are established by means of (re-)authentication protocols according to the 802.1x security model. Mainly, the DSAs are used to deploy security services upon a hop-by-hop security model (for authentication, integrity and confidentiality of data plane packets).

For the specification of the functional components interaction, we considered the scenario illustrated in Figure 1, where a new mesh node (denoted here SMSG-R) is joining the BAN mesh network. In order to support intra/inter-domain handover applications the interactions run according to HOKEY [7],[9] standard. Therefore, the SMSG-B is additionally assigned the re-authentication server role (a.k.a. ERP server).

In the case where the SMSG-R enters the network for the first time (i.e. it has no security context updated), it will be authenticated and authorized through the complete authentication procedure run with the SMSG-B within home domain, via SMS-B as authenticator. If SMSG-R is a visitor of the current BAN domain, the local SMSG-B shall play the role of a proxy F-AAA server. Otherwise, SMSG-R has already been (re-) authenticated and (re-) authorized within another BAN domain (i.e. it has updated security context) and subsequently will be re-authenticated and reauthorized at the current BAN using our optimized re-authentication procedure (specified in the next section), via SMS-B authenticator. This time, the local SMSG-B shall play the role of the re-authentication server. To assure proper operation of our re-authentication protocol a security context pre-distribution protocol shall run on the interface between local SMSG-B (F-AAA module) and home SMSG-B (H-AAA module). In the case of a successful (re-) authentication, the supplicant module located on SMSG-R and the authenticator module located on the physical adjacent SMS-B entity will run a legacy authentication protocol (e.g. "4-way Handshake") to check each other the claimed identity and establish a new DSA for securing the radio link that connects them. Eventually, the SMS-B is instructed by the SMSG-B to grant connectivity services to the SMSG-R entity.

3 SMART-Net Re-authentication Protocol

In this section, we specify a new authentication protocol optimized to support real-time applications during the handover process. It is designed to run in between the mobile node/subscriber (e.g. SMSG-R) and the re-authentication server (SMSG-B). The main objectives of our re-authentication protocol are:

- mutual authentication of principals;
- authentication key (material) synchronism verification and notification;
- master session key establishment (MSK).

This protocol combines asymmetric with symmetric cryptographic techniques to benefit the advantages of both schemes. The paradigm for its performances is the use of symmetric cryptographic algorithms, for computing authentication mechanisms, with the authentication key derived using an asymmetric method with the overall properties outlined below.

The proposed re-authentication protocol (see Figure 2) belongs to the class of "challenge-response" protocols with the time variable parameter of type nonce (e.g. random number). Both of the principals generate independently a nonce value with two objectives: to guarantee the protocol messages are fresh and to contribute to the master session key establishment. The last is required to avoid the master session key control by one principal, to guarantee its freshness and to enable PFS property (Perfect Forward Secrecy). Optionally, the protocol messages can provide an identification mechanism for principals, which is useful for authentication key derivation method.

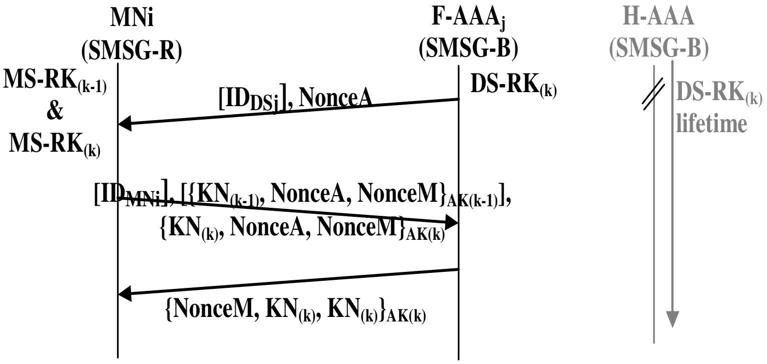
MNi
(SMSG-R)
F-AAA$_j$
(SMSG-B)
H-AAA
(SMSG-B)
MS-RK$_{(k-1)}$
&
MS-RK$_{(k)}$
[ID$_{DSj}$], NonceA
DS-RK$_{(k)}$
DS-RK$_{(k)}$
lifetime
[ID$_{MNi}$], [{KN$_{(k-1)}$, NonceA, NonceM}$_{AK(k-1)}$],
{KN$_{(k)}$, NonceA, NonceM}$_{AK(k)}$
{NonceM, KN$_{(k)}$, KN$_{(k)}$}$_{AK(k)}$

Fig. 2. the SMART-Net re-authentication protocol

In order to assure continuity of the re-authentication service during the re-authentication key management procedure, our protocol was designed to operate simultaneously with two successive authentication keys, associated to the time intervals (k-1) and (k). Moreover, each authentication key is assigned an identifier, named KN (k-1) and KN (k) respectively, to be used by the key re-synchronization mechanism. The identifiers are uniquely defined and distributed by the authentication server located in the home domain of the SMSG-R (see the next section). This way, if either authentication component {KN(k-1), NonceA, NonceM}_AK(k-1) or {KN(k), NonceA, NonceM}_AK(k) is valid (see the second message), then SMSG-B entity declares the SMSG-R as genuine. Each key identifier points to the authentication key to be used for validation of the corresponding authentication component. On the other side, SMSG-R relies on the last message to check the SMSG-B entity is authentic.

The first identifier in the last message points to the authentication key used by SMSG-B and the second identifier notify the SMSG-R about the most recent authentication key known by SMSG-B. Whenever the SMSG-R finds out this way a new authentication key have been established it starts (in parallel with the user data transfer) a complete authentication procedure with the authentication server in home domain, in order to obtain this key. If none of the authentication keys is known by SMSG-B, the protocol fails and the SMSG-R shall initiate the complete authentication procedure with the authentication server within the home domain. The transmission of the last message in this case is optional since its integrity cannot be verified.

After successful mutual authentication, the master session key can be derived independently by principals according to the following formula:

$$\text{MSK (k)} = \text{hash (NonceA, NonceM, AK(k))}$$

Thereafter, the MSK (k) is securely transferred toward the authenticator entity (typically an access point) and eventually the legacy local authentication protocol is run in between SMSG-R and SMS-B.

The Re-authentication Key Cryptographic Derivation Procedure

The real-time inter-domain re-authentication solution we proposed in this paper relies on the pre-distribution technique of the authentication key material from home domain to each subscriber entity (e.g. SMSG-R) and re-authentication server (e.g. SMSG-B) within each potential visited BANs, before the arrival of the mobile subscriber entity. The main hurdle to overcome was the issue of figuring out in advance what is the next visited BAN; and vice-versa, what is the next visiting mobile subscriber.

The key idea was to decouple to some extent the authentication key material from (subscriber entity, re-authentication server) pair. Therefore, we defined two components for deriving the authentication key: generic key material (generated and distributed by home domain authentication server) and local key material (known locally, such as identifiers of the principals). The main advantage of using generic key material is that it can be pre-distributed to all re-authentication servers and subscribers, before any tentative of association. Moreover, while the aim of the generic key material is to ensure the authenticity of the derived key and to supply the entropy, the local key material cryptographically binds the resulting authentication key to some (subscriber, re-authentication server) pair. In addition, a special cryptographic derivation method has been defined.

For maintaining the derivation method independent from the underlying cryptographic mechanisms, we will not specify in detail this method, but we point out below its overall design requirements:

- the authentication key derived has sufficient entropy to guarantee the required security level;
- the derivation transformation has one-way property;
- to guarantee the peer entities shall independently compute the same authentication symmetric key;

- (to prevent impersonation attacks) to guarantee the generic key material of some entity (subscriber or re-authentication server) cannot be used to compute neither the generic key material nor the authentication key corresponding to another entity or pair (subscriber, re-authentication server), respectively.

For a given pair of principals, we denote MS-RK and DS-RK the generic key material of the subscriber and the re-authentication server respectively. Further, we have considered the principals' identification information, denoted IDMN and IDDS as the local key material. Therefore, assuming the values of MS-RK, DS-RK, IDMN and IDDS are defined within the domain Zn, we have searched to figure out two functions f and g such that the following holds:

$$f, g : Z_n \times Z_n \rightarrow Z_n ,$$
$$g(f(RAND, IDDSj), IDMNi) = g(f(RAND, IDMNi), IDDSj)$$

where f is the generic key material derivation function MS-RK = f(RAND, IDMNi), DS-RK = f(RAND, IDDSj). RAND is a random value parameter in Z_n. g is the authentication key derivation function: AK = g(MS-RK, IDDSj) = g(DS-RK, IDMNi).

Re-authentication Key Material Distribution

Since the DS-RK key material is used by re-authentication server to compute the authentication key of all subscribers of the same home domain, its lifetime is critical. Consequently, the DS-RK is periodically updated by the authentication server in the home domain of those subscribers. A secured AAA protocol can be used to push this key material toward all target domains. The period of DS-RK update depends on the cryptographic mechanisms involved by the authentication key derivation transformation, and the frequency of its use. Once the DS-RK is updated, the MS-RK key material should also be updated. In this regard, the re-authentication server is responsible to notify (through re-authentication protocol) the subscriber SMSG-R about the new MS-RK. Subsequently, the subscriber we'll start the complete authentication procedure to pull the MS-RK directly from the authentication server within home domain. Therefore, a counter-based mechanism for key material identification was defined. Thus, each time a new generic key material is generated, also the new value of the counter is associated with that material, denoted KN(k). To ensure the authentication service continuity while keeping the authentication key distribution mechanisms simple, both the subscriber SMSG-R and the re-authentication server SMSG-B shall maintain always only the two most recent generic key materials. On the other side, the distribution of the local key material may take place directly between the principals. In our implementation, we assumed a re-authentication protocol mechanism for such a distribution of the principals' identification information. Alternatively, any legacy lower layer mechanism may be used, optionally with identity confidentiality guarantees if required.

4 SMART-Net Re-authentication Protocol Security Properties Validation

We chose to use AVISPA (Automated Validation of Internet Security Protocols and Applications) simulation-based tool for verification of the security properties of the SMART-Net AA protocol we designed. The AVISPA tool was developed within the European funded research project AVISPA [24], and comprises a suite of applications for building and analyzing EFSM-based (Extended Finite State Machine) formal models of security protocols that are specified using HLPSL (High-Level Protocols Specification Language) language. The AVISPA tool allows to easily achieve fully automatic security properties verification using four complementary formal assessment techniques, implemented by the back-ends analyzers it comes with: OFMC (On-the-Fly Model Checking), CL-AtSe (Constraint-Logic-based Attack Searcher), SATMC (SAT-based Model Checker) and TA4SP (Tree Automata-based analyzer for Security Protocols).

In this regard, we have built the formal model of the re-authentication protocol behavior. Thereafter, we specified the security requirements in terms of authentication and confidentiality goals. Since the HLPSL is a role-based language, we had to specify the actions of each authentication principal as a module, but the attacker that is predefined, according to the Dolev-Yao model [3] (i.e. it is capable to drop, replay, delay, decrypt/encrypt and forge packets by mean of the inferred keys). The simulation assumptions were: all the communications are carried out through attacker participation, the attacker can act as an intermediate entity (e.g. MITM attack model) or as a peer entity, the cryptographic/hash algorithms are known by the attacker (see Kerckhoff's principles), the identities and location of the principals are known to the attacker. As a result of the re-authentication subsystem analysis, we have defined two more representative simulation scenarios:

−*mobile mesh node knows two successive (valid) re-authentication keys (AK(k-1) and AK(k));*
−*mobile mesh node knows a single (valid) re-authentication key (AK(k))*

At the time this paper was written, the HLPSL formal model we built had already been assessed according to the inter-domain handover scenario proving that our re-authentication protocol can successfully fulfill the security goals. In other words, our re-authentication protocol is SAFE with respect to: the secrecy of the session key (formalized as confidentiality goal on AK (k)) and the replay threats (formalized as authentication message goals on temporal variables).

5 Conclusion and Future Work

This paper presents the preliminary results of a (re-)authentication protocol and its architecture design, developed for hybrid wireless mesh networks. We presented the main design requirements that enabled our solution to sustain real-time inter-domain handover re-authentication applications. Our approach relied on the pre-distribution of the re-authentication key material and the key derivation method, in order to decrease the inter-domain re-authentication latency at the values similar to the local intra-domain solutions. The overall properties of the key derivation transformation have been outlined. At the moment of writing this paper, an AVISPA-based simulation model of the re-authentication protocol had already been built and the preliminary security properties verification has been successfully passed.

The ongoing future work is to build an OPNET/NS2 simulation model to evaluate the proposed security architecture and related mechanisms' performance, in terms of delay and traffic overhead (i.e. scalability). Since the identification mechanism provided by our re-authentication protocol cannot guarantee the confidentiality of principals' identity, new solutions are presently researched to overcome this issue.

Acknowledgements. The authors would like to thank the European Commission for funding our research work in the framework of the SMART-Net project IST-2008 223937-STREP.

References

1. Wendt, S., Kharrat-Kammoun, F., Borcoci, E., Cacoveanu, R., Lupu, R., Hayes, D.: Network architecture and system specification, SMART-Net project IST-FP7 223937 (October 2009)
2. Menezes, A., van Oorschot, P., Vanstone, S.: Handbook of Applied Cryptography. CRC Press (October 1996)
3. Dolev, D., Yao, A.: On the security of Public-Key Protocols. IEEE Transactions on Information Theory 2(29) (1983)
4. Calhoun, P., Montemurro, M., Stanley, D.: Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Specification, IETF, RFC 5415 (March 2009)
5. Komarova, M.: Fast authentication and trust based access control in heterogeneous wireless networks, Ph.D. Thesis (May 2008)
6. Mishra, A., Shin, M., Arbaugh, W.: An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process
7. Clancy, T., Nakhjiri, M., Narayanan, V., Dondeti, L.: Handover Key Management and Re-Authentication Problem Statement, IETF, RFC 5169 (March 2008), http://www.ietf.org
8. Narayanan, V., Dondeti, L.: EAP Extensions for EAP Re-authentication Protocol (ERP), IETF, RFC 5296 (August 2008), http://www.ietf.org
9. Hoeper, K., Ohba, Y.: Distribution of EAP based keys for handover and re-authentication, IETF, draft-ietf-hokey-key-mgm-06 (April 2009), http://www.ietf.org
10. Clancy, T.: Secure Handover in Enterprise WLANs: CAPWAP, HOKEY and 802.11r
11. Huang, P.J., Tseng, Y.C.: A Fast Handoff Mechanism for IEEE 802.11 and IAPP Networks
12. Chen, J.J., Tseng, Y.C., Lee, H.W.: A Seamless Handoff Mechanism for IEEE 802.11 WLANs Supporting IEEE 802.11i Security Enhancements
13. Bournelle, J., Laurent-Maknavicius, M., El Mghazli, Y., Giaretta, G., Lopez, R., Ohba, Y.: Use of Context Transfer Protocol (CXTP) for PANA, draft-ietf-pana-cxtp-01 (March 2006), http://www.ietf.org

14. Ohba, Y.: Pre-authentication support for PANA, draft-ietf-pana-preauth-06 (June 2009), http://www.ietf.org
15. Forsberg, D., Ohba, Y., Tschofenig, B., Yegin, A.: Protocol for carrying authentication for network access (PANA), RFC 5191 (May 2008), http://www.ietf.org
16. Lupu, R., Borcoci, E., Mirzadeh, S., Hamadani, E., Rasheed, T.: D3.5a: Security and Privacy Requirements, SMART-Net project IST 223937 (April 2009)
17. Farell, S., Volbrecht, J., Calhoun, P.: AAA Authorization Requirements, RFC 2906, IETF (August 2000)
18. Aboba, B., Beadles, M.: The network identifier, RFC 2486, IETF (January 1999)
19. Vollbrecht, J., Calhoun, P., Farell, S., et al.: AAA Authorization Framework, RFC 2904, IETF (August 2000)
20. Lupu, R., Stanciu, M.: Authentication and authorization architecture for hybrid mesh networks. In: Conf. Int. Communications 2010 (Iunie 2010)
21. Long, M., Wu, C-H., David Irwin, J.: Localized Authentication for Wireless LAN Internetwork Roaming
22. Lin, X., Ling, X., Zhu, H., Ho, P.H., Shen, X.: A novel localised authentication scheme in IEEE 802.11 based wireless mesh network. Intl. Journal Security and Networks 3(2) (2008)
23. Hong, Z., Rui, H., Man, Y.: A novel fast authentication method for mobile network access (2004)
24. AVISPA, http://www.avispa-project.org
25. IEEE-SA Standards Board, Port-based Network Access Control, IEEE Std. 802.1x-2001 (October 2001) ISBN 0-7381-2626-7