END-TO-END SECURITY ESTABLISHMENT THROUGH OPERATORS: SIP EXPERIMENT

Afsaneh Yaghoobian, Maryline Laurent
CNRS Samovar UMR 5157, TELECOM SudParis, 9 rue Charles Fourier, 91011 Evry, France
Maryline.Laurent@it-sudparis.eu

Kourosh Teimoorzadeh, Jean-Philippe Wary
SFR, 1 Place Carpeaux, 92915 Paris La Défense, France

Keywords: Mutual Authentication, Secure Communications, C2C security, Multi-capacity Device, SIP.

Abstract: This paper proposes to experiment a secure multimedia session establishment in a fully open environment like Internet. Users equipped with multi-capacity devices can benefit from the authentication support of their operators to mutually authenticate, and secure their exchanges. Multi-operator crossed authentication can also take place under a previously signed agreement. In this paper, a SIP experiment with integration of SIM-based authentication is successfully conducted, thus demonstrating the feasibility of the end-to-end security establishment approach through operators.

1 INTRODUCTION

Until recent years, most of the multimedia applications and devices were proprietary with their own session protocol and security systems. Now, with the growing trend towards IP convergence (voice, data, video) and interoperability, the mobile phones can chat with computers whatever their access network and technology. This openness to media, networks and technology brings a number of security issues, like impersonation, theft of personal data, and man in the middle.

This paper is focusing on end-to-end mutual authentication and multimedia data flow security. In (Wary and Laurent, 2009), we proposed an approach to benefit from each original network authentication procedure provided by the operators (e.g. a cellular network operator, an Internet Service Provider…) in order to support mutual authentication between two subscribers. Subscribers are only assumed to be equipped with multi-capacity devices (3G, Bluetooth, ad hoc, Internet…) and to have Internet connectivity. They benefit from the high-level security offered by their operators to establish a secure channel. This solution is independent of the underlying technology in use. It is also adapted to multi-operator crossed authentication through signed agreement in between. In (Wary and Laurent, 2009), concepts were fully described, but no instantiation of them was proposed.

In this paper, we demonstrate the feasibility of this secure approach by integrating a SIM-based authentication into the most famous multimedia session establishment: SIP (for Session Initiation Protocol). The advantage of this secure SIP approach over the standardised IMS (IP Multimedia Subsystem) AKA authentication is that users are not required to subscribe any IMS service. They can initiate any SIP service from any service provider. They can make use of the authentication service currently provided by their own operators. SIP users only have to agree on using a compatible SIP software client.

This paper is organized as follows. Section 2 introduces the mutual and flexible authentication approach as described in (Wary and Laurent, 2009), and section 3 the SIP protocol standard with flows. Section 4 presents our technical choices for the selection of the authentication method, and the integration of the authentication procedure into SIP exchanges. Section 5 details our SIP experiment. Finally, section 6 gives conclusions, and discusses

related issues before the operators can charge this authentication service to subscribers. Acronyms are listed at the end of the paper.

2 MUTUAL AND FLEXIBLE AUTHENTICATION SUPPORTED BY OPERATORS

The approach to support a bidirectional and flexible authentication of users is deeply described in (Wary and Laurent, 2009), and is summarized in this section.

2.1 Assumptions

The assumptions of our solutions are as follows (see figure 1 for notations):

- The Entity-A is a subscriber of Operator-A, and Entity-B to Operator-B. The Operator-A is used to authenticate Entity-A on network access technology T#1, and the Operator-B is used to authenticate Entity-B on access technology T#2. The Entity-A is uniquely identified by the Operator-A with the following NAI (Network Access Identifier): Entity-A@Operator-A. The Entity-B is uniquely identified by Entity-B@Operator-B.
- Entities A and B are equipped with multi-capacity devices, and at least one of the interfaces of the device is common (technology T#3) for the entities to exchange their data traffic. The device of Entity-A has the following available technologies T#1, T#3 and T#5, and the device of Entity-B is provided with interfaces of technologies T#2, T#3 and T#4.
- Entity-A is authenticated over the technology T#1 by Operator-A, and Operator-A can generate several Authentication Vectors AV_A (available in the Operator-A's infrastructure T#1) to support some authentication of Entity-A. AV_A includes a pre-computed session key $SSK_{B=>A}$.
- Entity-A is authenticated over technology T#5 to Operator-A to the Authentication Gateway AG(A). A secure channel over (SSK_A) is established between Entity-A and AG(A).
- Entity-B is authenticated over the technology T#2 by the Operator-B which is then able to generate a set of vectors AV_B for subsequent authentications of Entity-B. AV_B includes a pre-computed session key $SSK_{A=>B}$.

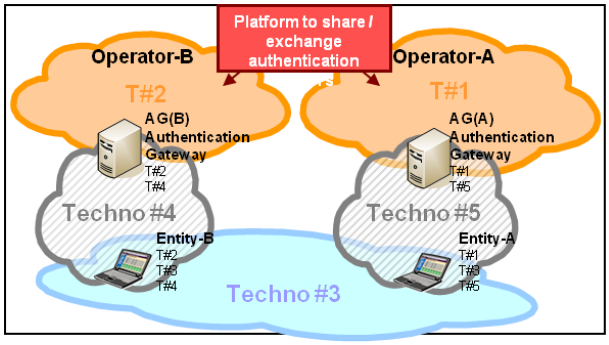

Figure 1: Architecture of our authentication approach.

- Entity-B is authenticated to AG(B) over the technology #4, and a secure channel over (SSK_B) is established between Entity-B and AG(B).
- Operators A and B have previously signed an agreement to offer a crossed authentication service to their subscribers and/or to provide mutually requested Authentication Vectors to their Authentication Gateway. As such, AG(B) is able to get AV_A from AG(A) for the specific customer Entity-A. Likely, AG(A) gets AV_B from AG(B) for Entity-B. Note tha this type of agreement is already in use today between 2G and 3G Mobile Network Operators in order to provide international roaming to their mutual customers. In this case, the legacy network and technology used to exchange these authentication vectors is the SS7 network and protocol.

2.2 Secure communication establishment

Entity-A and Entity-B can mutually authenticate and establish a secure communications based on the following steps:

- Entity-B invites Entity-A over technology T#3 to establish a session and supplies its identity Entity-B@Operator-B to Entity-A.
- Entity-A requests directly AG(A) (over T #5) for Entity-B@OperatorB's authentication vectors.
- AG(A) requests Operator-B for specific authentication vectors ($AV_{A=>B}$) for Entity-B@Operator-B customer.
- AG(A) sends back to Entity-A (T#5) the vector $AV_{A=>B}$ and the way to proceed to the authentication of Entity-B.

- Entity-A authenticates Entity-B and if successfully done, it provides to Entity-B its identity (over T#3): Entity-A@Operator-A. Otherwise, Entity-A closes the session. At this step, Entity-A and Entity-B share a secret value ($SSK_{A=>B}$).
- Entity-B requests AG(B) (T#4) for the authentication vectors of Entity-A@Operator-A.
- AG(B) requests Operator-A for the authentication vector for Entity-A@Operator-A customer.
- AG(B) sends back to Entity-B $AV_{B=>A}$ (T#4).
- Entity-B authenticates Entity-A. If successfully done, Entity-B and Entity-A share two secret values ($SSK_{A=>B}$) and ($SSK_{B=>A}$).

- At this stage, Entity-A and Entity-B mutually authenticated and are then able to bootstrap (over T#3) a security protocol in between, i.e. based on a common session key. The security protocol can be initialized based on a session key ($SSK_{A/B}$) computed by each party with the shared secret values ($SSK_{A=>B}$) and ($SSK_{B=>A}$). Note that the secret of these keys is guaranteed as they were exchanged through secure channels (SSK_A) and (SSK_B) through T#4 and T#5 technologies.

3 SESSION INITIATION PROTOCOL

The Session Initiation Protocol (SIP) is an IETF protocol (Rosenberg et al., 2002) that supports multimedia session establishment (VoIP, videoconferencing, streaming multimedia…) using text-based (HTTP-like request/response) signaling messages. SIP became of high importance in 2000 when it was integrated into 3GPP (3rd Generation Partnership Project) signaling protocols as part of the IMS (IP Multimedia Subsystem) architecture elements for multimedia streaming in cellular devices.

3.1 Functional elements

The SIP architecture includes several entities:

- User Agent (UA): The Internet endpoints of SIP session like SIP phones. UAs are participants to the SIP session. One is generating SIP requests and the other is returning responses. The role of UA last for the duration of the SIP transaction only.
- Proxy server: The proxy servers are intermediary entities during SIP session establishment. They help the UA to locate and route the SIP call to the appropriate UA. They can also deny or authorize call establishment, and they handle registrations, invitation sessions, and other SIP requests.

3.2 SIP flows

As standardised in (Rosenberg et al., 2002), the establishment of a multimedia session from Entity-A with Entity-B works as follows (see figure 2). Entity-A first transmits an INVITE message (F1) to its own SIP proxy server (domainA.com) which identifies the SIP proxy server of Entity-B (domainB.com). The INVITE message is then routed through the identified server (F2) to Entity-B (F4). The F3 and F5 100 Trying responses are notifying the senders of F1 and F2 messages that their request is being moved toward the destination.

As soon as F4 message is received, Entity-B's SIP phone starts ringing and Entity-A is notified that the invitation has been received with the 180 Ringing message (F6) going through the SIP proxy servers (F7, F8).

The next messages are generated when Entity-B accepts the call, i.e. he picks up the phone. A success 200 OK message (F9, F10, F11) is then sent to Entity-A. It makes the phone stop ringing and Entity-A immediately sends an acknowledgement message (ACK F12). Note that the previously exchanged SIP messages are all going through the SIP proxy servers, except the ACK F12 message which goes directly from Entity-A to Entity-B. This is made possible thanks to Entity-B's IP address which is communicated to Entity-A in the 200 OK message.

At any time later, Entity-A or Entity-B can close the connection sending a BYE (F13) message followed by a returned acknowledgement OK (F14).

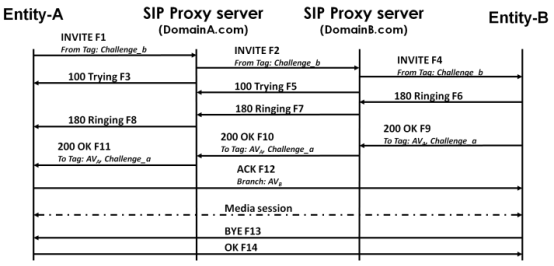

Figure 2: SIP flows enriched with Authentication Vectors.

4 TECHNICAL CHOICES FOR SECURING SIP WITH OPERATORS SUPPORT

Our idea is to enable two SIP entities to securely authenticate to each other by exchanging their authentication vectors through SIP messages over the T#3 network technology (cf. figure 3), whatever the security level of access network technology T#3 (cellular, WiFi…). That is, the SIP Proxy servers are located on the T#3 network. To verify the validity of its remote SIP peer, the SIP entity forwards to its operator (Operator-A for Entity-A, and Operator-B for Entity-B) the received authentication vector of the peer through T#4 or T#5 technology. Operator-A and Operator-B under a previously signed agreement are thus asked to perform two one-way authentications. There must be no ambiguity about the linkage between users' identities: the one used by operators to perform the authentication (e.g. IMSI of SIM cards), and the one used by SIP Entities within SIP exchanges (e.g. string).

4.1 Selection of the authentication method

Several authentication methods like EAP-SIM (Haverinenet et al., 2006), EAP-AKA (Arkko and Haverinen, 2006), and EAP-AKA' (Arkko and Lehtovirta, 2009) are suitable for our SIP experiment. They all consider the network access operator as a major actor of the process. The operator can issue several authentication vectors for a subscriber to later support offline authentications of them. Also they can delegate the authentication of their subscribers to other parties by transmitting the authentication vectors. One has only to pay attention to not afford replay of authentication vectors. Management of them must be very strict.

We selected EAP-SIM as it is widely used in the GSM mobile phone networks. It offers a strong authentication level thanks to the SIM card provided with the mobile phones. We adapted the EAP-SIM challenge/response method to our SIP architecture and identification scheme, for simplification and performance reasons. As such, we only consider the SIM authentication vector made of the following triplet:

- RAND: a random number ;
- SRES: result which is computed over RAND value and a secret key only known by the SIM card and the operator;
- Kc: a confidential key.

Adaptation of the SIM-based authentication to our bidirectional authentication need is performed as illustrated in figure 3. Entity-A is assumed to have first contacted Operator-B (through its gateway) to get AV_B. Entity-A then extracts the RAND value and sends it to Entity-B. Entity-B then generates the SRES result with its own SIM card, and sends it back to Entity-A for verification. For mutual authentication support, Entity-B has to request AV_A from Operator-A (after getting identity of Entity-A) and proceeds the same way as A. Once the authentication is successully done, both entities Entity-A and Entity-B are sharing two confidential keys $SSK_{A=>B}$ and $SSK_{B=>A}$ (see section 2.2).

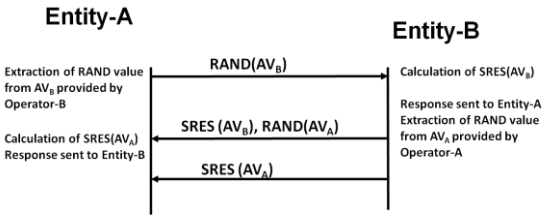

Figure 3: Simplified SIM authentication method.

4.2 Integrating authentication elements into SIP messages

To perform the simplified SIM authentication over a SIP session establishment, we identify the best SIP fields where to inject the authentication elements of figure 3. We decided to integrate directly the authentication elements into the existing SIP session establishment messages (INVITE, 200 OK, ACK). There was another option that uses NOTIFY and INFO optional messages which can be exchanged at any time between SIP entities. However, it was not selected for performance reasons not to slow down too much the authentication procedure, and SIP

session establishment. Also, this option assumes that the authentication is well synchronized with the SIP session setup, so in case of authentication failure, the session setup is denied. Note that the NOTIFY and INFO option is of interest for authentication support if the authentication procedure requires more than three-way exchange.

We make use of the random content fields Tag and Branch to carry the authentication information elements as illustrated in figure 2. The Tag field is available in From field of INVITE message and serves to carry the first authentication element (RAND value of AV_B as given in figure 3). The Tag field is also available in To field of 200 OK message and is used for carrying SRES of Entity-B and RAND(AV_A). The Branch field is available in Via field of the ACK message, and carries the SRES value of entity-B. The advantages of this solution are of twofold. First, their content is usually set by the SIP initiator end-point and is randomly generated, as such replacing this value with a random extracted from the vector does not disturb the basic SIP establishment procedure. Second, these fields are interpreted by end SIP entities only, so we are sure that intermediary proxy servers will not modify them during transfer.

Referring to the mutual authentication presented in section 2, we assume that all the required assumptions are satisfied. As such, at the very beginning of the authenticated SIP session, Entity-A and Entity-B are authenticated to their own operators Operator-A and Operator-B. Entity-A then asks for the authentication vector of Entity-B to Operator-A. Thanks to some agreement with Operator-B, Operator-A communicates AV_B to Entity-A. Entity-A then sends an INVITE message to Entity-B including RAND(AV_B) in From Tag. Upon receiving the INVITE, the From Tag is parsed, and the RAND value serves to generate the SRES of Entity-B. Entity-B extracts the identity of Entity-A from the From field and requests an authentication vector AV_A from Operator-A, like Entity-A did previously. Entity-B then forges the 200 OK message with its SRES result, and the random value RAND(AV_A) into To Tag field. Entity-A checks that the received SRES matches the SRES field of AV_B. Then it calculates its SRES result using RAND(AV_A) provided by Entity-B, and sends it back to Entity-B in Via Branch field of ACK message. In case the authentication fails, Entity-A or Entity-B can close the session.

5 SIP EXPERIMENT

Our SIP experiment is a first step for proving that SIP can be secured by introducing lightweight extra authentication information elements into SIP session initiation messages.

5.1 Material and environment

The platform is made of two Windows XP x64 PCs, and a Windows XP laptop. All three equipements are belonging to the same network, and to the same SIP proxy domain. The PCs are running the SIP clients (Express Talk softphone), and the laptop is running the proxy server shared by the SIP clients. The SIP server is an open-source software from Brekeke: OnDoSIP Server (based on Java J2SE JRE 1.4 and Servlet Engine Apache Tomcat 4.1.2). All the developments were done in Java with NetBeans IDE 6 .7.1 programming environment.

5.2 Results

Both SIP clients are statically configured with some predefined SIM authentication vectors, so no extra communications with operators are required.

The SIP clients are modified to exchange authentication information elements in their INVITE, 200 OK, and ACK messages. For the SIP initiator (Entity-A), the instance `s` of the *Sender* class (Express Talk softphone client) that generates session initiation messages is modified as follows:

```
   s.from = "entitea"; //Anything but
not empty
   s.to = "entiteb"; //the name of the
callee registered into the proxy server
   s.realm = proxy;
   s.fromtag = "sim01rand_b";
   s.ipsender = "157.159.16.106";
```

The `From Tag` field is set to **`"sim01rand_b"`** to inform the receiver Entity-b that the SIM method applies and this is the first message of the authentication procedure. The returned 200 OK message carries the information **`"sim02resp_b_rand_a"`** in the `To Tag` field and the ACK the **`"sim03resp_a"`** in the `Via Branch` field.

The tests performed successfully. Appropriate authentication elements entered lead to a successful SIP session establishment, and otherwise to closing the session.

5 CONCLUSIONS AND DISCUSSIONS

This paper demonstrates through a SIP experiment how users could benefit from the strong authentication procedure provided by their operators. For the operators, this approach can be easily deployed at no huge extra cost, as the security material is already available in the terminals. For SIP software editors, this is a new opportunity to introduce security into multimedia applications, even in unsecure network environments (i.e. Interne). Of course, integrity protection of these multimedia clients must be ensured, e.g. to make sure the strict control over the authentication vector usage is not compromised.

As the targeted market for such end-to-end authentication service is huge, and the service requires resources, there is a high interest for operators to charge this authentication service and get a new significant source of revenue. One solution for billing the service would be to charge a subscriber each time he/she is requesting an authentication vector, for authenticating a newly contacted person. The charging might also vary depending on the complexity of the authentication protocol, as the higher the security level, the greater the demanded resources.

ACRONYMS

AG	Authentication Gateway
AV	Authentication Vector
SIM	Subscriber Identity Modules
SIP	Session Initiation Protocol
UA	User Agent
UAC	UA Client

REFERENCES

Arkko, J., Haverinen, H., 2006. Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA). In *IETF RFC 4187*, Informational.

Arkko, J., Lehtovirta, V., 2009. Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA'). In *IETF RFC 5448*, Informational.

Haverinenet, H. et al., 2006. Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM). In *IETF RFC 4186*, Informational.

Rosenberg, J. et al., 2002. SIP: Session Initiation Protocol. In *IETF RFC3261*, Standards Track.

Wary, J.-P., Laurent, M, 2009. Secure communications between multi-capacity devices with authentication support by network operators. In *MWNS 2009, Workshop on Mobile and Wireless Networks Security*, Aachen, Germany, pp25-35.