Secure communications between multi-capacity devices with authentication support by network operators

Jean-Philippe Wary[1] and Maryline Laurent-Maknavicius[2],

[1] SFR, 1 Place Carpeaux,
92915 Paris La Défense, France
[2] CNRS Samovar UMR 5157, TELECOM&Management SudParis,
9 rue Charles Fourier, 91011 Evry, France
{jean-philippe.wary@sfr.com, Maryline.Maknavicius@it-sudparis.eu}

Abstract. This paper proposes to benefit from each natural network authentication procedure provided by operators to allow mutual authentication between two multi-capacity devices and guarantee the same security level to both of them. Operators can agree providing jointly this authentication service so multi-operator crossed authentication infrastructures can take place for instance over internet. As such, users needing strongly secure interconnectivity (e.g. SIP usage or over ad hoc infrastructures) can access to this service through Internet with no huge extra costs contrary to PKI or Kerberos solutions. Additionally to this attractive marketing offer, authentication could become a new growth for operators.

Keywords: Key Agreement, Mutual Authentication, Device Pairing, Secure Pairing, Multi-Capacity Devices.

1 Introduction

In several situations, users through their terminals need to mutually authenticate and secure data traffic across a wireless communication channel. IP telephony is one of these applications where users would like to establish a voice call at low cost over Internet but with security and privacy guarantees. They want to be sure that their correspondent is as claimed, and their communications will not be eavesdropped. File sharing over Internet, or over an ad hoc network is another example where the identity of the entities must be guaranteed and the data exchanged need confidentiality and integrity protection. All these applications require opportunistic communications to be initiated with high-level security.

The arrival of multi-capacity devices on the market brings diversity in terms of technological means (3G, Bluetooth, ad hoc, Internet…), and the nature of the interconnection which might be direct between two devices or performed across a network. The intermediary network, if any, can be infrastructureless (e.g. ad hoc network) or under the supervision of an operator (e.g. 3G). Due to the wide variety of their features, the network access technologies have very different security levels, ranging from a weak level (Bluetooth) up to a strong level (3G). The usage of multi-capacity devices thus brings more flexibility to users as crossed technology combinations may help solving the security session establishment between devices.

A number of security solutions were published in the last few years in order to help any pair of devices getting into contact for the first time to interconnect securely. A first pairing approach relates to devices close to each other (i.e. in the same radio coverage) that need auxiliary channel(s) for transmitting an authenticated secret for next securing their direct exchanges. Other approaches are under the assumption of an existing trusted third party like Kerberos, Wireless PKI (WPKI) or an AAA service. Most of them are mono technology solutions, i.e. having the same network interface enabled to perform both security establishment and traffic exchange.

This paper proposes a new approach that benefits from the natural network authentication procedure performed by the operators (e.g. a cellular network operator, an Internet Service Provider…). Any subscribers having Internet connectivity are able to mutually authenticate, and secure their communications, whatever the underlying interconnection technology in use. This approach has several advantages. Deployment of it is easy and no huge extra cost is needed as the security material is already available in the terminals. Multi-operator crossed authentication is made possible. Both users benefit from the high-level security offered by the operators. Finally, for operators, the authentication service itself can be a new source of income.

The organization of the paper is as follows. First, section 2 presents related works and highlights the need for designing a new C2C (Customer-to-Customer) oriented approach. Section 3 describes the network architecture and clarifies the prerequisites of our approach. Section 4 gives the conceptual description of the approach and section 5 concludes.

2 Related works

In the past five years, a number of research and standardization works were conducted on how to initiate a secure session between any two users (i.e. their devices) getting into contact for the first time. They do not know each other and they do not share any common context (e.g. pre-shared key). Beyond the authentication problem, the session key establishment problem raises. According to the underlying network technology, several approaches were investigated.

2.1 Secure pairing approaches

The pairing approaches relate to devices that are in the same short-range radio coverage, and can directly interconnect. Bluetooth and Wi-Fi are two examples of our everyday life needs in direct and close interconnectivity. In the literature [1], the security approaches rely on some auxiliary physical channel(s) that can be authenticated by the users, and serve to communicate some secrets. The originality of the approaches lies in the nature of the channel that is classically visual, audio, touch… and based on the devices' available features such as LEDs, beeping, vibration, or any synchronized combination of them. Usually the users are asked to proceed to the validation of the channel by comparing character strings, the good synchronization of light/sound/vibration signals on both devices… In some cases, users support the synchronization itself by putting closely together the devices in a certain position or shaking the devices together [2]. The relevance of the secure pairing approaches can be measured by their user-friendliness, the rate of false negatives, and their rapidity of execution.

2.2 Trusted third party approaches

Other approaches are under the assumption of an existing and online trusted third party like Kerberos, Wireless PKI (WPKI) or AAA service, but these approaches are B2C oriented only. They permit a customer to authenticate to a service or network provider, but they do not solve the C2C connectivity security problem. Even if Kerberos [3] could be pretty easily adapted to C2C communications, it is very heavy in terms of number of exchanges and CPU processing. Kerberos requires that users are previously known to one of the Kerberos servers and it does not fit to the inter-domain authentication.

The AAA service [4] is an internal service used by operators to authenticate their subscribers with a high level security before affording them access to their networks. With the Diameter protocol [5], inter-domain authentication between operators is possible, but as it is standardized and used today, this AAA authentication service can't be accessed by any other external entity. Some research efforts are in progress in

that direction to help users establishing secure communications over ad hoc networks thanks to some delegated AAA ad hoc nodes [6] or a distributed AAA service [7].

Finally, WPKI [8] is adapted to mobile users that need to authenticate to a service provider (mainly e-governmental and banking services) or to sign a document. The online WPKI service of the cellular network operator is acting as a proxy between the users and the service providers, handling the authentication of the users based on private/public key. The WPKI provides a unidirectional crossed-technology authentication, with the user asking for a service access from a terminal (e.g. PC) and performing unidirectional authentication from his cell phone. The resulting authentication level is the one provided by the operator and SIM card usage.

2.3 Approach [9]

The approach [9] is also worth presenting as it considers a crossed technology authentication based on mobile phone authentication. From a PC, a user can authenticate to any Internet application server with the help of an online identity provider belonging to the cellular network operator. The identity provider helps the user to download java applets on the PC, so the PC can locally access to some SIM USB dongles, or locally communicate to his cell phone through Bluetooth. This authentication is unidirectional, B2C oriented, and does only support mobile phone authentication.

2.4 Strong need for designing a new authentication approach

None of today's authentication approaches support all the following features:

- mutual authentication with the same level of authentication for both parties;
- crossed-technology authentication, the multi-capacity device can operate authentication on one of its enabled interface and handle data traffic on another interface;
- inter-domain and multi-technology authentication, so any subscribers of operator A using access network technology T#1 can authenticate to any subscribers of operator B with technology T#2;
- C2C, C2B and B2C authentication, any entities having the capability to authenticate to any operators can be authenticated by any other entities.

To simplify and strengthen security in C2C, C2B or B2C communications, and prepare a secure and open environment for next coming applications, there is a strong need to develop a new authentication framework and protocols. The next section describes the objectives of our proposed authentication approach and the observed constraints.

3 Architecture, prerequisites and constraints

The objective of our approach is to provide a bidirectional and flexible authentication service offering a possibly large choice of authentication methods, with no high extra cost for the operators and users, with a symmetrical approach for the authentication handling.

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.
- The 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.

- The 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 (for instance AG(B) is able to request an authentication vector for a specific customer of Operator-A)[i].
- The Entity-A is naturally authenticated over the technology T#1 by the Operator-A, and there is another type of authentication over the technology #5 realized by the Authentication Gateway AG(A). For this service, AG(A) naturally uses the authentication vector (AV) computed by Operator-A[ii] using the technology T#1.
- In the same way, the Entity-B is naturally authenticated over the technology T#2 by the Operator-B, and there is another type of authentication over the technology #4 realized by the Authentication Gateway AG(B). AG(B) uses likely some authentication vectors (AV) available in the Operator-B's infrastructure (T#2).

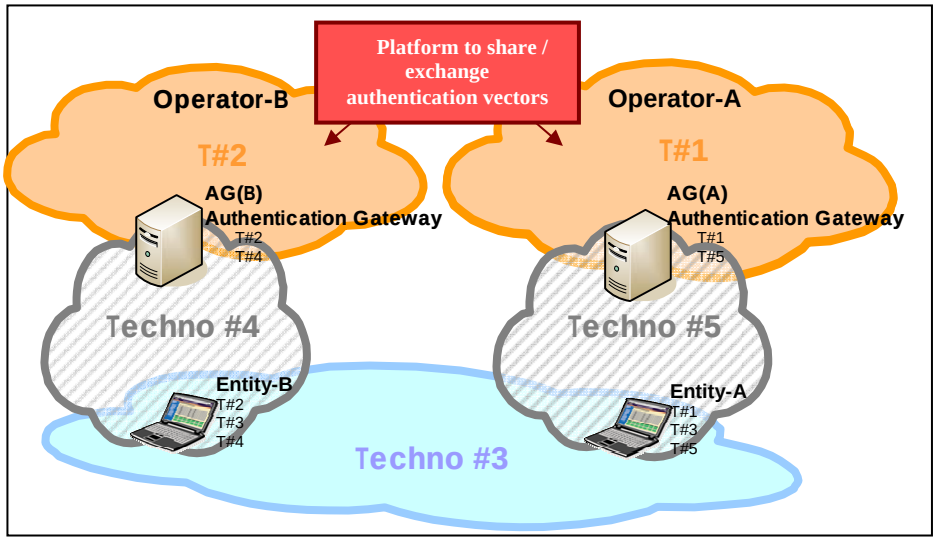

Figure 1: Architecture of our authentication approach

The EAP authentication methods can provide a shared secret that might serve to bootstrap a security protocol between entities A and B.

4 Description of the concept

This section is organized in four parts:

- A simple way to extend EAP-AKA usages over Internet,
- A generalization of the mutual authentication concept,
- Identification of open issues, in particular regarding the potential gradient of trust regarding authentication methods available to each entity.

[i] 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 natural network and technology used to exchange these authentication vectors is the SS7 network and protocol.

[ii] For instance, the Operator-A may be a Mobile Network Operator using the 3G technology (T#1), in this case the authentication vector to be supplied to AG(A) to authenticate the Entity-A over internet (technology T#5) is naturally based on EAP-AKA protocol definition and the Entity-A is authenticated by AG(A) with the EAP-AKA protocol.

4.1 A simple way to extend EAP-AKA usages over Internet

We illustrate in a simple way the concept through the usage of EAP-AKA (Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement) [10] which is the natural authentication method to be implemented between AG(A) and the Entity-A.

In this example, the Entity-A is authenticated by AG(A), which has requested the necessary authentication vector to the native MNO operator (on which the Entity-A is regularly registered, it means that Entity-A has some SIM card issued by Operator-A). In case of success of the EAP-AKA authentication phase, the two parties AG(A) and Entity-A then share the same set of secret keys: a 128 bits session key for integrity check (IK_A) and a 128 bits session key for encryption (CK_A). The two parties are then able to build a secure channel with (IK_A) and (CK_A), and only those two parties are able to know the values of the two keys (IK_A) and (CK_A). It means that every packet can be ciphered with these keys and the other party, is the only one (already authenticated) able to use and know the secret key to decipher the packets.

This technology is currently deployed by MNO operators to offer Wi-Fi access to their customers without any extra access control scheme.

In our case, it is now possible to have a simplified view of the general case, if we consider that:

- The two Entities A and B are owned by the same Operator-A (for instance a 3G MNO),
- The Entity-A is already sharing a secure channel with AG(A) over Internet (it means that AG(A) already authenticated Entity-A through the EAP-AKA protocol),
- The Entity-B is not connected on Internet, but is connected to an ad hoc network (technology T#3) on which Entity-A is already connected.

As discussed in the state of the art, if Entity-A shares its Internet access with the ad hoc network, then Entity-B may establish a secure channel with AG(A) through the EAP-AKA protocol (all the communications will be routed by Entity-A).

Our proposal is that Entity-A plays the role of AG(A) regarding Entity-B to allow Entity-A to authenticate Entity-B by requesting AG(A) (with which Entity-A already shares a secure channel based on a first EAP-AKA challenge), the necessary authentication vectors (for EAP-AKA protocol) computed in the infrastructure of the Operator-A. At the end of this second EAP-AKA challenge, the Entity-A will have authenticated the Entity-B with the level of trust provided naturally by the 3G Authentication protocol and it will share with Entity-B the keys ($IK_{A=>B}$) and ($CK_{A=>B}$).

It means that any 3G customer is able to authenticate “strongly” any other 3G customers over ad hoc technology as long as it is able to communicate with its Authentication Gateway AG(A) (through SMS or Internet access for instance). The authentication is qualified as strong since the challenged customer is using its SIM card to answer to the EAP-AKA Challenge, and today 3G Mobile Network Authentication are not repudiable or broken.

It has to be noted that over the ad hoc network, Entity-B is able to authenticate Entity-A by replaying the same protocol with AG(A) (AG(A)= AG(B)):

- The authentication of Entity-B to AG(A) routed by Entity-A over Internet,
- Entity-B requests an Entity-A’s authentication vector (EAP-AKA protocol) to AG(A),
- The authentication of Entity-A by Entity-B over the ad hoc technology through the received EAP-AKA protocol based on the AG(A) received authentication vectors.

At this moment, Entity-A and Entity-B share four 128 bit keys:

- From the first step when Entity-A authenticates Entity-B: ($IK_{A=>B}$) and ($CK_{A=>B}$),
- From the second step when Entity-B authenticates Entity-A: ($IK_{B=>A}$) and ($CK_{B=>A}$).

4.2 A first level of generalization of the mutual authentication concept

We illustrate the generalization of the concept with the following hypothesis:

- H1: Entity-A is already authenticated (EAP-AKA protocol) by the Authentication Gateway AG(A) through the technology T#4 and a secure channel over (IK_A) and (CK_A) is already established between Entity-A and AG(A).
- H2: Entity-B is already authenticated (by a proprietary "weak" algorithm based on a password hashed with a random challenge) through technology T#5 by Authentication Gateway AG(B) and a secure channel over a session key (KS_B, computed by the derivation of the password with a random value) is already established between them.
- H3: Entities A and B are able to communicate over a dedicated technology #3, which naturally does not provide security features.
- H4: The two Operators A and B are able to exchange authentication vectors through a dedicated mean. Operator-A supplies to AG(B) some EAP-AKA authentication vectors, and Operator-B supplies to AG(A) some proprietary authentication vectors (which may be composed of: Random-Value, RES_B: Result of a first hashing function applied to the customer password and the Random value, a session key: KS_B the result of a second hashing function applied to the customer password and the Random value).
- H5: The Entity-B wants to establish a secure session with the Entity-A over the technology T#3.

The following steps apply:

- Entity-B invites the Entity-A to establish a session and supplies its identity Entity-B@Operator-B to Entity-A,
- Entity-A requests directly AG(A) for Entity-B@Operator-B authentication vectors,
- AG(A) requests Operator-B for specific authentication vectors AV_B for the customer Entity-B@Operator-B,
- AG(A) sends back to Entity-A the necessary information and the way to proceed to the Entity-B's authentication,
- Entity-A authenticates Entity-B and in case of success, it provides to Entity-B its Identity: Entity-A@Operator-A (in other cases, Entity-A may close the session). At this step, Entity-A and Entity-B share the values: Random-Value, RES_B, KS_B . KS_B is a secret value which is not exchanged over the technology T#3,
- Entity-B requests AG(B) for Entity-A@Operator-A's authentication vectors AV_A,
- AG(B) requests Operator-A for specific authentication vectors for Entity-A@Operator-A's customer.
- AG(B) sends back to Entity-B the EAP-AKA authentication vector ($AV_{B=>A}$),
- Entity-B authenticates Entity-A. If successful, Entity-B and Entity-A share the secret values: ($IK_{B=>A}$) and ($CK_{B=>A}$). Otherwise, Entity-B may close the session.
- At the end, Entity-A and Entity-B have proceeded to a mutual authentication and are able to build a secure channel between them based on this mutual authentication. The secure channel may be based on a session key $SSK_{A/B}$ computed by each party with the following shared secret values: KS_B, $IK_{B=>A}$ and $CK_{B=>A}$.
- The use of a shared secret key $SSK_{A/B}$ is equivalent to an implicit mutual authentication, because only the other already authenticated party may be able to use and know the secret key $SSK_{A/B.}$

To generalize the concept, we have no hypothesis on the available authentication methods for each technology, we only consider that each of these methods allows the operators to compute and supply authentication vector (AV) that may contain the necessary information to proceed to a one-way authentication and in case of success, it establishes a session key SSK.

4.3 A second level of generalization of the mutual authentication concept

The assumptions of the section 3 apply, and have to be completed with the following hypothesis:

- H1: Entity-A is already authenticated by Authentication Gateway AG(A) and a secure channel over (SSK_A) is already established between Entity-A and AG(A).
- H2: Entity-B is already authenticated by Authentication Gateway AG(B) and a secure channel over (SSK_B) is already established between Entity-B and AG(B).
- H3: Operator-A is able to provide AV_A to GA(B) on request, and AV_A includes a pre-computed session key: ($SSK_{B=>A}$).
- H4: Operator-B is able to provide AV_B to GA(A) on request, and AV_B includes a pre-computed session key: ($SSK_{A=>B}$).
- H5: Entities A and B are able to communicate over a dedicated technology #3.

The following way to build a mutual authentication between the parties A and B:

- Entity-B invites the Entity-A to establish a session and supplies its identity Entity-B@Operator-B to Entity-A,
- Entity-A requests directly AG(A) 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 the necessary information ($AV_{A=>B}$) and the way to proceed to the authentication of Entity-B,
- Entity-A authenticates Entity-B and if successful, it provides to Entity-B its identity: Entity-A@Operator-A. Otherwise, Entity-A may close the session. At this step, Entity-A and Entity-B share a secret value: ($SSK_{A=>B}$) which was not exchanged over technology T#3,
- Entity-B requests AG(B) for Entity-A@Operator-A authentication vectors,
- AG(B) requests Operator-A for specific authentication vectors ($AV_{B=>A}$) for Entity-A@Operator-A customer,
- AG(B) sends back to Entity-B the authentication vector ($AV_{B=>A}$),
- Entity-B authenticates Entity-A. if successful, Entity-B may close the session. Entity-B and Entity-A share two secret values: ($SSK_{A=>B}$) and ($SSK_{B=>A}$) which were not exchanged over technology T#3,
- At this stage, Entity-A and Entity-B proceeded to a mutual authentication and are able to build a secure channel between them based on this mutual authentication. The secure channel may be based on a session key ($SSK_{A/B}$) computed by each party with the following shared secret values ($SSK_{A=>B}$) and ($SSK_{B=>A}$),
- The use of a shared secret key $SSK_{A/B}$ is implicitly equivalent to a mutual authentication, as the other party (already authenticated) is the only one able to use and know the secret key ($SSK_{A/B}$).

Mutual authentication between two parties is thus achieved over the technology (T#3) by using the existing infrastructures and the native security services provided by their native Operators.

4.5 Open issues

Several open issues are identified:

- How to manage the fact that the operators A and B may provide different levels of security and trust in their native authentication scheme for their customers? Is it possible to clearly evaluate/measure the level of the provided mutual authentication if operators offer dissymmetric levels of security for their own customers' authentication?
- Is it possible to define a way to manage at each entity's level an Information Security Policy to protect internal assets in case of dissymmetric level of authentication during the mutual authentication phase?
- This scheme is a new way of growth for operators by charging delivery of authentication vectors. A new billing scheme similar to the transportation of voice might emerge with payment by the entity requesting the authentication vector or the entity doing the checking. On which bases can the operators build a new revenue scheme?
- Is it possible to easily extend this mutual authentication between two entities to some group authentication ? This will be helpful to secure the access to some multicast applications and their multicast data.

5 Conclusions

This study allows any customers to authenticate mutually over any technologies as long as they still be able to communicate with a trusted entity, i.e. their native home operator. The interesting point is that the proposed concept doesn't need any costly investment as it completely reuses existing technologies and platforms (EAP-AKA, HSS and GBA for Mobile network operator, EAP-TLS and each existing EAP method).

As we demonstrated, if one of the parties is only protected by a login/password technology [11], the secure channel established with another party using a SIM card improves the security of the channel and the mutual authentication between the parties. Improvement is high in comparison to the weak security level offered by the use of password technology.

We are convinced that there is a huge interest today regarding the 3 billion SIM cards used over the world to secure mobile network communications, in particular if they can be reused by customers to communicate over unsecure networks. The use of these authentications, as described in this paper, might strongly help to support secure mutual authentication in a number of communications scenarios over the world.

A patent application has been filed in August 2008 (under the number FR 0855595).

References

1. Saxena, N., Voris, J.: Pairing Devices with Good Quality Output Interfaces. **In:** Distributed Computing Systems Workshops, 2008. ICDCS '08. 28th International Conference on, pp. 382--387 (2008)
2. Castelluccia, C., Mutaf, P.: Shake them up!: a movement-based pairing protocol for CPU-constrained devices. In: Shin, K.G., Kotz, D., Noble, B.D. (eds.), Proceedings of the 3rd International Conference on Mobile Systems, Applications, and Services. MobiSys 2005. pp. 51--64. Seattle, Washington, USA (2005)
3. Neuman, C., Yu, T., Hartman S., Raeburn, K: The Kerberos Network Authentication Service (V5), IETF Request for Comment 4120 (2005)
4. C. de Laat, Gross G., Gommans L., Vollbrecht J., Spence D.: Generic AAA Architecture, IETF Request for Comments RFC2903 (2000)
5. Calhoun, P., Loughney, J., Guttman, E., Zorn, G., Arkko, J.: Diameter Base Protocol. IETF Request for Comments RFC3588 (2003)
6 Chaouchi, H., Laurent-Maknavicius, M.: Toward a New ad hoc node design for secure service deployment over ad hoc network. In: Workshop on Mobile and Wireless Networks Security. MWNS 2008. pp. 1--11, Singapore (2008)
7 Larafa, S., Laurent-Maknavicius, M., Chaouchi, H.: Light and Distributed AAA Scheme for Mobile Ad hoc Network. In: First Workshop on Security of Autonomous and Spontaneous Networks. SETOP 2008. pp. 93--104. Loctudy, France (2008)
8. WAP Forum: Wireless Application Protocol, http://www.wapforum.org
9. Van Do, T., Jonvik T., Feng B., Van Thuan D., Jorstad I.: Simple strong authentication for Internet applications using mobile phones, In: IEEE GLOBECOM 2008. New Orleans, USA (2008)
10. Arkko, J., Haverinen, H.: Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA). IETF Request for Comments RFC4187 (2006)
11. Blunk, L., Vollbrecht, J., PPP Extensible Authentication Protocol (EAP), . IETF Request for Comments RFC2284 (1998)