SIM-Mee - Mobilizing your social network

Jérémie Albert, Serge Chaumette, Damien Dubernet, Jonathan Ouoba

HAL Id: hal-00411204
https://hal.science/hal-00411204

SIM-Mee
Mobilizing your social network

J. Albert, S. Chaumette, D. Dubernet, and J. Ouoba,

LaBRI, Université Bordeaux 1
Contact author : serge.chaumette@labri.fr

Introduction

Social Networks such as LinkedIn or FaceBook offer the opportunity to set up a group of friends or professional relationships .In such systems, the interaction most of the time takes place through a central Web site that can be accessed from a browser or from a mobile phone. In some sense the relationship thus remains virtual, disconnected from the real world. *SIM-Mee* bridges the gap between social networks and the real world, by making it possible to discover and interact with the members of your own network who happen to be geographically close to you in the real life, still ensuring privacy.

From a technical point of view, it illustrates the convergence of several technologies (NFC, SAT, SCWS, Bluetooth) inside a single community oriented service. *SIM-Mee* relies on the secure exchange of virtual business cards, including signatures, each card being stored in the USIM of its owner's mobile phone. Exchanging cards is achieved in a contactless secure manner (by using NFC), by touching one phone with the other. Based on these cards and signatures, *SIM-Mee* offers a mobile social networking service in which a *SIM-Mee* user is able to discover those of his friends (i.e. the persons of who he owns the virtual business cards) who are in his neighborhood. The list of discoverable friends and the list of friends the user agrees to be discovered by are manageable through and address book like system (by means of a Servlet embedded in the USIM).

This system can be used for instance in a train or an airport. One can select the persons he agrees to talk with, and if they are also present in the train/airport then both parties will receive a message saying that they are close to each other. They will then be able to initiate a classical call/text message and eventually meet somewhere in the train/airport.

Main features and underlying technologies

The main features that are supported are:

Business card management (uses SAT, SCWS and NFC): The necessary support to edit and exchange business cards is provided. The edition of the user's personal business card takes place through a SAT[1] menu while the other cards are displayed using an embedded web application (SWCS[2]). The cards are exchanged by NFC[3].

Security and privacy (uses asymmetric cryptography[4]): Security and privacy are achieved by using asymmetric cryptography. Each user is provided with a pair of secret/public keys. His public key is part of his business card, while its secret key remains in his USIM card. It makes it possible to authenticate a user and to cipher communication.

NFC power off: We have added a feature to put the application (more precisely its applet part) in « power off mode » in order to prevent a business card from being caught by any reader without the authorization of its owner. Without this feature, as soon as a mobile phone would get in reach of any reader, it would respond to any request to exchange its business card, which is highly intrusive.

Discovery of contacts: The discovery of contacts makes it possible to work contacts of a user (the persons of which he have a business card) who are in his geographical area. This is achieved in a secure way by using the keys associated to each user (the public key of a user being part of his business card).

High level architecture

As explained above and show figure 1, *SIM-Mee* illustrates the convergence of different technologies. From a practical point of view, it consists of two parts: first, a Java Card Applet[5] which provides secure transfer (using NFC) and storage of business cards, and business card management (using the USIM embedded Smart Card Web Server[2]); second, a J2ME MIDlet[6] that makes it possible for a user to discover those of his contacts who are in his neighbourhood.
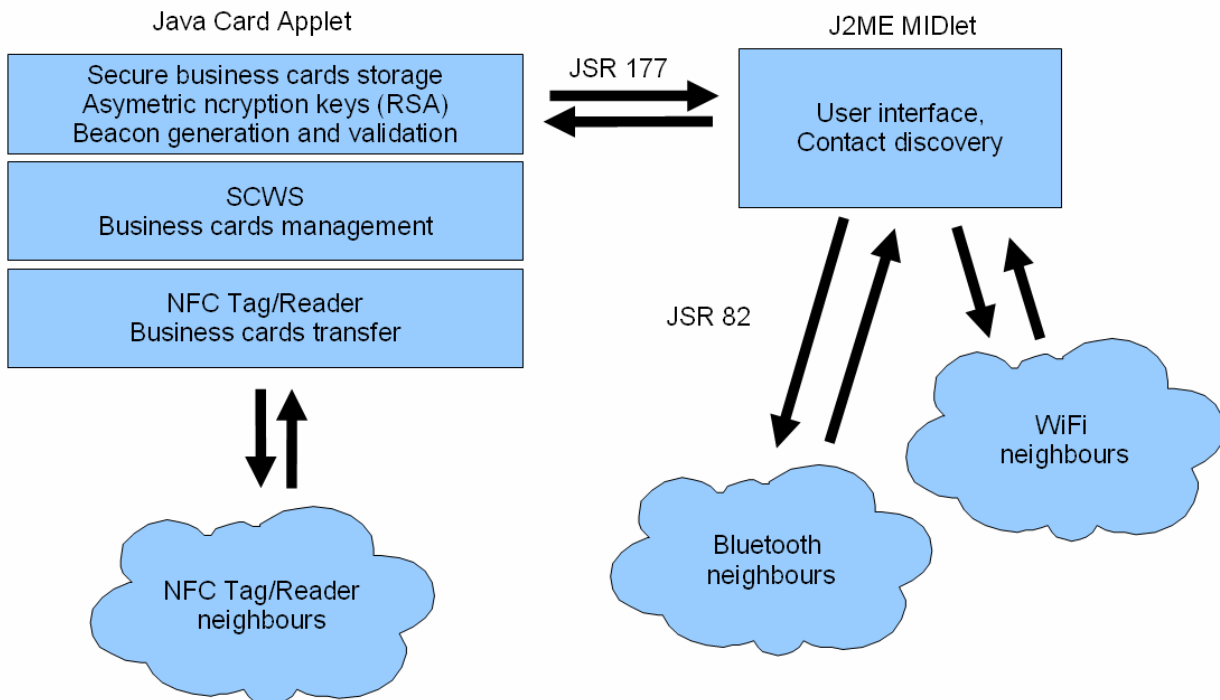

Figure 1- The global architecture of SIM-Mee

Usage scenario and security considerations

In this section we assume two mobile phones, A and B, and explain the interactions that take place between the different components of the *SIM-Mee* architecture, i.e. the applet, the MIDlet and the user of both A and B. These interactions rely on the following pieces of information:

- Applet (of mobile) A knows: its own phone number; a pair of secret/public keys : SK_A and PK_A; the phone number of (mobile) B; the public key of B: PK_B.
- Applet (of mobile) B knows: its own phone number; a pair of secret/public keys: SK_B and PK_B; the phone number of (mobile) A; the public key of A: PK_A.

Phase 1. Business Card Management and Exchange

A user creates his business card (that will be stored in the USIM of his phone) by providing his name and his first name. The phone number that is also part of this business card is retrieved from the USIM card.

Once this card has been created it is possible to exchange it with another phone. To achieve this process, the user must set his NFC enabled phone in tag mode. The second phone involved in the process must be set in reader mode (more precisely its NFC chip) to receive the card. The two phones need to be physically put close to one another for the communication to take place.

It should also be noted that *SIM-Mee* makes it possible to manage the business cards stored in the local USIM through the embedded Smart Card Web Server. When the web server is launched with the proper parameters (address, port and application name), a web page containing the business cards stored in the USIM are displayed and can be managed.

Phase 2. Contact Discovery

It is now possible to send an announcement message to discover those persons listed on the contact list who are present in the neighbourhood. This process relies on a MIDlet which communicates with the applet (to acquire the contact list, and for message encryption/signature)) via APDU commands (through the JSR 177[7] API). The MIDlet uses Bluetooth[8] to communicate any reachable contact.

For example assume user A wants to check if used B is around.

User A, who is running MIDlet A on his mobile phone, selects user B in his contact list and initiates the neighbourhood search. Let us recall that PK_A and PK_B respectively stand for the private key of user A and user B, as stored in their USIM.

MIDlet A locally retrieves the message $M1 = PK_B(phone\_number\_A, random1)$ from Applet A and sends it to its neighbours. The neighbours are all the available Bluetooth devices that host the SIM-Mee service. The nounce *random1* is used to prevent replay.

If user B is in the neighbourhood, Midlet B receives M1 and forwards it to applet B for verification purpose. Applet B deciphers message M1 (the other neighbours will not be able to decipher it and will thus ignore the message and will consequently neither be discovered nor be aware of the presence of A) and verifies that user A is in the set of persons B wants be visible for. If it is the case, applet B returns a message $M2 = PK_A(phone\_number\_B, random1, random2)$ to MIDlet B. The nounce *random2* serves the same purpose as *random1* above.

MIDlet B sends M2 to MIDlet A via Bluetooth and at reception the message is forwarded to Applet A. Applet A verifies that M2.random1 is equal to M1.random1. If it is true, applet A returns $M3 = PK_B (telephone\_number\_A, random2)$ to MIDlet A.

At this stage, if Midlet A gets M3, it displays a message to inform user A that user B is nearby. M3 is also sent via Bluetooth to Midlet B.

MIDlet B forwards M3 to Applet B. Applet B verifies that M2.random2 is equal to M3.random2. If this is true, applet A returns a code meaning that user A is a neighbour, and Midlet B can display a message to inform user B that user A is nearby.

Users A and B now know that they are close to each other and can decide on meeting.

The other devices in the neighbourhood receiving M1 are not alerted since they are not the target of the announcement message (they work that out because the announcement message is ciphered with PK_B).

Conclusion

SIM-Mee, as a social networking application, corresponds to a real demand of the users. It bridges the gap between social networks and the real world, by making it possible to discover and interact with the members of your own network who happen to be geographically close to you in the real life (still ensuring privacy). You can mobilize your social network at the airport, at the station, in the train, in the subway, in a nightclub, in a school, etc.

SIM-Mee is easy to deploy because it does not require any infrastructure. The applets and MIDlets can be downloaded on the phones that are already deployed.

Using *SIM-Mee* is free (but using *SIM-Mee* will arouse calls and text messages (SMS). Furthermore, future extensions will generate additional traffic, for instance business cards could be updated by using text messages. We are also working on a formal validation of the security of the whole system using Avispa[9].

References

[1] USIM/USAT support
   http://www.accessdevnet.com/index.php/ACCESS-Linux-Platform-Native-Development/ALP_Telephony_MobileServices.html#1013158

[2] SWCS: Smart Card Web Server
   http://www.gemalto.com/france/telecom/

[3] NFC: Near Field Communication Handbook
   Syed A. Ahson, Mohammad Ilyas, Borko Furht
   Auerbach Publishers Inc.

[4] Applied Cryptography
   Bruce Schneier
   Wiley, 2nd edition

[5] Java Card applet developer's guide
   http://www.javaworld.com/javaworld/jw-07-1999/jw-07-javacard.html?page=1

[6] The Java Micro Edition technology
   http://java.sun.com/javame/technology/index.jsp

[7] JSR 177: Security and Trust Services PAI for J2ME
   http://jcp.org/en/jsr/detail?id=177

[8] Bluetooth
   http://www.bluetooth.org

[9] Analysing Security Protocols with AVISPA
   Laura Takkinen
   Helsinki University of Technology