Advanced SIM capabilities supporting Trust-based applications*

Thomas Vilarinho[1], Kjetil Haslum[2] and Josef Noll[3]

[1] Department of Telematics at NTNU and Telenor R&I, Trondheim,
tcarlyle@gmail.com
[2] Telenor R&I, Trondheim, kjetil.haslum@telenor.com
[3] University of Oslo/UNIK, N-2007 Kjeller, josef@unik.no

Abstract. The SIM cards are going through several new enhancements both in the underlying hardware and its capabilities. They are becoming secure wireless networked devices containing embedded sensors. This paper assess how this new capabilities together with the pervasiveness and security of the SIM card can support the development and design of trust-based applications. Moreover, we present a specific use-case around a seamless trust builder for social networks, which makes use of sensed inputs towards building hard contextual evidences to trust relations. We conclude with the description of the challenges of building this evidence based trust-builder and the necessary steps to going from the prototype we developed to a real application which may accurately describe trust relations.

Keywords: SIM cards, trust, networked embedded systems, pervasive computing, Sun SPOT, social networks, context-awareness.

1 Introduction

It is unanimous that the mobile phone is the most popular personal pervasive device so far. The strong presence of mobile phones, together with the development of new interfaces and sensors, has pushed several applications to be developed on this platform. However, the mobile phone itself is not considered a platform truly secure as it seldom has memory access protection or physical tampering sensors. On the other hand all mobile devices represented by the Global System for Mobile communication (GSM), which corresponds to more than 80% of the mobiles[4], have a security element represented as the Subscriber Identity Module (SIM) card.

The SIM, as a smart card, corresponds to a well trusted and tamper-proof device. Smart cards are trusted enough to play key roles in highly secure business cases such as banking, key management, identification and authentication. Using

* This is a post-peer-review, pre-copyedit version of an article published in Lecture Notes in Computer Science, vol 5838. Springer, Berlin, Heidelberg. The final authenticated version is available online at: https://doi.org/10.1007/978-3-642-04766-4_16

[4] http://www.gsmworld.com/newsroom/market-data/market_data_summary.htm

the SIM instead of the Trusted Platform Module (TPM) has the advantage of having a physical element which the user can remove. Thus it offers the possibility for identity mobility, as the identity of the device (through the SIM) can be moved from one device to another device.

Besides the access to all features from the mobile or from any other device to which the SIM card is connected, new physical and logical interfaces are becoming available to the SIM. Standard and non-standard wired and wireless interfaces and sensors are being integrated to the SIM. In addition to that, we are starting to see more and more cases of multi-application cards. These new capabilities being developed around the SIM, allied with its pervasiveness and security, enable it to play different new roles, such as: a trust component for federated identities, a secure platform for the Internet-of-things, a seamless provider of contextual evidences, or a mix of those.

On the other hand the phenomenon of online social networks (OSN) has also reached an enormous number of users. Their popularity is so big that about 20% of the Internet page views currently are from the social networks MySpaces and Facebook, where this corresponds to half of the views between the top 10 most popular domains, [1]. Facebook, in 2009, had more than 200 million active users where half of them access it at least once a day, while MySpace reported more than 110 million active users in 2008. Those two Social Networks together have more active users than the whole population of the United States, the third most populated country in the world.

However, the relations established in those social networks are not representative enough for serving as a base to attribute the trust between users that have a relationship defined there. Breslin and Decker point out that in many OSNs people connect to each other for only boosting their number of connections [1]. Moreover, several users feel compelled to accept friendship invitations despite they would not do it in the real life [2]. A survey done with some users of the Orkut social network showed that about one fourth of the connections that those users have done was due to a feeling of an obligation, as users preferred to add an unwanted friend instead of possibly offending the person [3]. Due to the mentioned problems and the fact that those OSN relations often do not carry attributes that characterize them, it may be misleading to assume that one user trust the other, in a general or restricted context, based on those virtual relations.

We see that the new advanced features on the SIM card can offer a solution to the lack of trust in the user's connection in social networks. This future SIM can counter impersonification through mutual authentication mechanisms, but it can also seamless sense the real life interactions between the users and offer real hard evidences towards the description of the users' trust relations.

In this paper we asses some situations that could benefit from this new capabilities of the SIM, and describe the case of a transparent trust builder. This trust builder makes use of the identities stored in the SIM card and the context information acquired during the contact between two SIMs in order to characterize the trust relation between the two SIM card owners. We have developed a small prototype using Sun SPOTs emulating this future SIM card in the seamless trust building scenario. Despite using a simple trust logic and limited contextual information we achieve promising results and indications of what other factors could be modeled in order to reach a more accurate trust builder.

The rest of this paper is organized as follows. Section 2, we describe the state-of-art of the SIM cards and its applications on trust building; afterwards, we present the related work towards using the SIM to build trust and around categorizing relations. Then, in section 4, we explain the seamless trust builder and the experiments and results we achieved. In the final part of the paper we conclude with presenting directions of future work.

2 The State of the Art in SIM Card Technology

Thanks to the high rate of evolution in the telecommunications, SIM cards have leaded the advances of smart card functions. Their main function has been to prove the authenticity of the mobile device in respect to the network. But as theirs capabilities were expanded, they became the secure element for several applications, acting as identity and profiling devices for the user, and as a secure channel between theirs applications and the mobile phones.

One of the driving factors to the continuous raise of the importance of the SIM card is its security characteristics. Both hardware and software passes through rigorous development process, enforced by auditions and clear standards. Thanks to that process, the smart card industry manages to be ahead of the attacks that can be performed at lower cost than the value of the data secured in the card [4, 5]. Moreover, the smart cards offer a multi-application architecture where a firewall is established between the applications securing their execution and the data access. This is assured by the implementation of the Global Platform (GP) standards [6], and the concepts of the Card Manager and Security Domains.

SIM card applications such as JavaCard applets or SIM browsing, as Wireless Internet Browser (WIB) and S@T, use the SIM as a trusted platform in order to exchange messages via Over-the-Air (OTA) platforms. Those applications can be remotely loaded and managed, exchange messages and use cryptographic primitives through the security domains implemented in the SIM and standardized by the Global Platform specifications.

Those applications depend on the SIM Application Toolkit (SAT) to access the mobile phone capabilities, such as intercepting phone calls, sending messages, GUI methods, sensors and communication interfaces, such as Bluetooth and General Packet Radio Service (GPRS). The SAT specifies few interactions commands with the mobile, besides the management of logical channels between SIM and handset. However, in order to exchange large portions of data through those logical channels, both mobile phone and SIM need to implement a higher level data transfer protocol such as the Bearer Independent Protocol (BIP) or native TCP/IP protocol. So far, few handsets implement BIP and the native implementation of TCP/IP in the SIM cards has just been recently standardized by the European Telecommunications Standards Institute (ETSI) in [7].

J2ME applications running in the mobile can communicate with the SIM through the Security and Trust Services API for J2ME (SATSA); JSR 177. This API allows the J2ME Midlets to exchange Application Protocol Data Units (APDUs) with the SIM. By that, the Midlet can use the SIM to store keys and perform cryptographic operations such as digital signatures, encryption and authentication, as explored in [8]. A high level communication protocol between handset and SIM is the recent SIM Card Web Services (SCWS), specified in [9]. The SCWS enables the application in the SIM Card to be accessed through the terminal's browser, through BIP or TCP/IP, and to be managed through OTA.

A great breakthrough in the SIM cards has been the expansion of its communicating capabilities. The communication to the local reader has been improved from the 9.6 Kbits/s rate of the T=0 and T=1 protocols to around 8-12 Mb/s from the USB protocol. This is actually one of the driving factors for the development of higher bandwidth protocols in the SIM, such as the SCWS and the implementation of native TCP/IP. Besides the advances in the physical communication, recent releases from SIM cards producers such as Samsung and SanDisk have managed to deploy smart cards with powerful 32-bit processors and more than 1GB of memory.

Other interfaces are emerging around the SIM as well. The SIM pin that was used in the past for the programming voltage has become the connecting pin to the Single Wire Protocol (SWP), the physical link to a Near Field Communication (NFC) module standardized in [10, 11]. Moreover, Smart Card manufacturers and operators have announced the integration of accelerometer[12], GPS[13], IEEE 802.15.4 [14] and IEEE 802.11[15] interfaces directly on the SIM. All those interfaces grant to the SIM a high level of connectivity and context awareness independent of the terminal capabilities. Furthermore, ETSI has been working on standards to specify SIM cards that have more robust physical characteristics, targeting the machine-to-machine (M2M) market, as evidenced in the 3GPP M2M feasibility study [16].

In order to comply with those hardware advances, the JavaCard, the most penetrated smart card platform, has just seen a major improvement in its specifications. The new JavaCard 3.0 release supports more classes and features of the Java SE, multithreading, nested transactions, annotations and it adds an unified naming scheme for both applications and theirs resources [17].

There are several examples of applications and projects using the SIM card we have nowadays as a trust element. Some examples are Digital Rights Management (DRM), Mobile-banking, one-time password (OTP) solutions, Biometric verification, unified authentication, etc. The current potential of the SIM towards a local identity manager is further discussed in [18]. This identity management is especially improved with the new hardware changes in the SIM, and it has triggered the specification of an Identity Management (IdM) Framework by the GSMA [19].

This IdM framework breaks the definition of the Identity Provider in Authentication Provider and Identity Attribute Provider. The Authentication Provider is responsible for validating the user's credentials and providing him authentication assertions. In contrast, the Identity Attribute Provider facilitates sharing user attributes to trusted parties.

There is a great speculation over this attribute sharing capability, as it could offer extremely valuable information for content customization since users seem to be willing more and more to share personal information, as observed in [20, 21]. Once the SIM card starts to aggregate the mentioned sensors and communication interfaces, it can fetch real time context attributes that could be eventually shared through this Identity Attribute Provider, enhancing even more the customization potential for Value Added Services. In fact, as a pervasive device which is almost always with the user, it becomes the perfect platform for this real-time context sensing.

The diversity of sensors and interfaces allows the deployment of a context characterization and quantification framework just as described in [22] and [23], where all the inputs are combined to generate a context value with its context quality parameters such as: freshness, accuracy, precision, reliability and granularity [24]. Or this diversity of sensors could lead to optimize the context acquisition in terms of use of sensors and consumed battery based on the desired threshold of context quality parameters.

This context and its attributes can be applied as hard evidences towards the user or object, in the M2M case, when building trust around that context. This hard evidence capability can be endorsed by an authentication by the user or physical mechanisms on the SIM to detect that it hasn't been physically tampered, as the logical isolation is already provided by the SIM operational system and its security domains.

The potential of context-awareness is enormous. The wireless interfaces and NFC enables the SIM to sense the surrounding devices. This, together with the fact that the SIM card carries at least one identity (the Mobile Subscriber ISDN Number), enables to sense the relation between people: how often do they meet, how long do their meetings last, and which activities do they perform together. Moreover, those SIM could sense the surrounding objects that share their attributes, not only RF-ID tags but possibly other wireless devices that offer web services to reachable devices. And, by that acquire more information about the surrounding environment.

3 Related Work

The SIM card already plays a role for building trust as it is used as the main component to the GSM Authentication in the GSM Networks. It corresponds to a complex case of Identity Management (IdM) and policy-based trust, as the subscriber can seamless roam in different networks as long as there is a roaming agreement between the operators, somehow similar to Single-Sign-On (SSO) case based on a federation agreement between Identity Providers. National ID cases, such as the FINEID (Finish ID), Austrian ID and MyKad (Malaysian ID) for example, have successfully deployed IdM solutions hosted on the SIM Card, thanks to its multiapplication and applet firewalling capabilities.

Despite the cases of building trust based on shared keys in the SIM and in the authority that issues those keys in order to perform identity management, mobile banking, authentication or controlling data access; we could not find any approach in the scientific literature towards sensing context with the SIM in order to characterize relations between people as in the seamless trust builder we have designed. In [25], Mayes et al discuss the potential of high density smart cards, but the article mainly focus on the high capacity and the increase of the speed in the physical interface of the SIM, not much on its potential as personal trusted context-aware platform. A framework for treating information from sensors connected to the mobile in order to generate a high level and quantified is presented in [22]. But, [22] does not go into the details of the usage of the context information

In the other hand, [26] and [27] tries to seamless characterize trust relations between individuals, but based on theirs distance in OSNs. It is a valid approach as long as those relations in those social networks carry attributes that make them meaningful. The characterization of those relationships with the focus on the mutual reliance between the users is something that the seamless trust builder aims to do.

4 The Seamless Trust Builder

As mentioned in the introduction, the relationships in online social networks (OSNs) do not truly characterize trust relationships between its users. The reason for that is the lack of attributed information on the OSN links to serve as base for representing how much and in which kind of situations one user would trust the other. As trust, we consider how much the user could rely on the other's willingness and capability to act as expected on situations like giving advices, providing a service, etc. In fact, some social networks, such as Facebook, are adding mechanisms to arrange friends on group categories. However, defining those groups in the current OSN demands a lot of engagement from the users. Thus, the seamless trust builder could sense evidences in the user relations and transparently categorize the relationship between the users, giving them real meaning and suitable for inferring the trust between users.

4.1 Contextual Evidences

Considering the whole conjunct of interfaces and sensors that have been so far announced we identified a few context and sensors that could be retrieved by this future SIM, as summarized in Table 1.

Theoretically it would even be possible to have access to other sensors in the mobile such as: camera, microphone, light sensors (commonly present for the camera) and temperature sensors (commonly present for battery monitoring), as noticed in [28]. However the temperature and light sensors are usually not open to be used by 3rd party applications and the camera and microphone may be too invasive or demand too much processing and storage.

Table 1. Sensors and contexts available for the SIM trust builder

Context	Sensing Interface	Availability
Location	GPS, CellId; or NFC, IEEE 802.15.4 and IEEE 802.11 for relative position	Embedded in either standard or prototype SIMs
Environment, or surrounding devices	NFC, IEEE 802.15.4 and IEEE 802.11	Embedded in either standard or prototype SIMs
Motion	Accelerometer or based on location over time	Embedded in either standard or prototype SIMs
Activity	Accelerometer to some extent or application in the mobile or SIM	SIM can host applications and communicate with apps on the phone
User Profile	User information in databases linked to his identities	SIM can hold several identities

Still, with the sensors listed in the table we can already acquire a great amount of information, especially if we consider the access to information stored in databases linked with the user's identity. Thanks to the facilitation to publish content provided by the Web 2.0, nowadays users leave several digital footprints in the web. Gathering those attributes (such as the home address of the user, his profession, interests, family tree, etc) can offer almost unlimited possible inputs to enrich the description and contextualization of his profile or a trust relation held with other users. It would be possible to infer if the users share common interests; have distinct or similar points of view; are family related; etc.

4.2 The seamless trust builder

In fact the seamless trust builder uses the SIM context-awareness at two different stages. First, to detect that two users are close to each other, as we infer that due to this proximity they share some kind of relation or interaction. Then, it retrieves information about the context where both users are, gathering the necessary inputs to describe the interaction between the users. Then, based on this mutual interaction, it attributes a trust value between them.

When reasoning about a situation where a user needs to assess its reliance in the other agent, he can take into account a recommended trust (based on the recommendation of trusted sources), a historical trust (based on previous similar situations) or his dispositional trust towards that agent. This dispositional trust is what the literature [29] refers as default trust behavior of the trusting agent, his basic tendency to rely on the other agent. And, it is the dispotistional trust that the trust builder aims to give a value to.

Native radio interfaces such as NFC, IEEE 802.15.4 and IEEE 802.11 would be enough to sense other future-SIMs in the radio range, as a proximity sensor. But, in order to protect the user's privacy, he must be able to decide to broadcast or not his identity. Moreover, if he does, he should be able to choose to identify himself through a pseudonym instead of his real name, or possibly have his pseudonym or identity dynamically chosen based on the context. A mutual authentication mechanism, such as the Transport Layer Security (TLS) handshake, could be first required in order that the SIMs exchange more information, as their pseudonym or even profile attributes. By that, it would be possible to correlate the context in the situation just in case the users have some trust level between themselves or between a common trusted authority.

Once the interaction is detected, it is time to sense the context information so it can be categorized and serve as an input to generate a trust value. Based on the previous section, we have identified the following inputs for describing the interactions: duration, timestamp, location, profiling, and the user's activity. The duration can be calculated by measuring the time elapsed since the moment where the users get in contact and separate from each other. The timestamp can be retrieved by the phone or network clock, while for the location there are several possible sensors. Some location sensor could provide an absolute location, based on a numeric coordinate cartographic system, or a symbolic location, such as in a shopping center, at home, etc. The profile attributes could be fetched through the user's identity and connection to the Identity Attribute Server of that identity.

The activity of the user is much harder to be categorized. First of all, because the user may be engaged in more than one activity simultaneously such as walking while talking in the mobile and watching an outdoor in the street. It is not so hard to sense the activities which are based on the mobile device, such as using a mobile application or talking on the phone, as this could be sensed by the SIM through the interfaces towards the mobile such as SAT, SCWS, JSR-177, etc. But for other activities, which are the ones the user spend most of his time, sensing them is much more complex. This complexity includes the difficulty to sense those activities and to describe them.

For the sensing for example, the accelerometer can track the user motion, but we would need to recognize the activity based on the movement pattern. As an example, a study done by Karantonis et al [30] tries to identify a few distinct user activities with focus on elderly monitoring. They try to recognize situations such as if the user is standing up, sitting, falling and walking. Although, they managed to detect with good accuracy the changes between activity and rest, the detection of the cases where the person was walking was not accurate.

On the other hand other contextual inputs can help to deduce the user activity. As for example, if it is sensed that he is moving, but inside a football field, there are more chances that he is playing football. However, it is common to find exceptions in most of the cases, as for example the goalkeeper would have very different moving patterns from an attacker, although both of them are playing football. This is mainly a problem on describing the activity and it can be sometimes countered by limiting the scope of activity characterization. The activity could be limited for example just as if the user is busy or idle.

Based on the mentioned inputs of activity, location, timestamp and duration sensing, it is necessary to deduce a trust value from it. As pointed out in [31], the majority of the current reputation systems do not differentiate between general trust and contextual trust although it is an important issue. A user may trust another about work related topics but not on personal issues. For our seamless approach, we can benefit from the sensor to help detecting the context. This motivated us to generate not a single dispositional trust value, but a few different contextual dispositional trust values. Those values could be later used to create a more advanced user social network representation or to automatize or improve decisions that rely on another user.

Most of the challenges towards attributing the right quantization of some contexts and the calculation of accurate trust values are closely related to pattern recognition whose root are in the sociology, psychology and cognitive sciences. However, in this paper we focus on the sensing capabilities and, consequently, we don't focus on the pattern analysis. We use a simple model and simple scenario in order to build a proof-of-concept application showing the potential of the SIM to become a passive trust builder in the future due to its sensing capabilities.

4.3 Implementation

As this paper explores the capabilities that are being developed on the SIM but are not yet present in a product available for developers, we decided to do our implementation in a Sun SPOT (Sun Small Programmable Object Technology).

The Sun SPOTs are small, wireless devices embedded with 3 different sensors (temperature, light and an accelerometer) besides I/O general purposes pins that enable the connection of additional sensors. The Sun SPOT hosts a small-footprint J2ME java virtual machine running directly over the hardware. The hardware consists of a 180 MHz 32 bit ARM920T core processor with 512K RAM and a 2.4 GHz IEEE 802.15.4 antenna. There are two types of Sun SPOTs: the free-range SPOTs which have all the sensors; and the basestation SPOT which does not have sensors (just the IEEE 802.15.4 interface) but can connect to a PC by USB port and serve as a gateway between the other SPOTs and the PC.

The Table 2 lists the pros and cons of using the Sun SPOT for emulating this future SIM.

Table 2. Restrictions in using the Sun SPOT for emulating an enhanced SIM

Advantages	Disadvantages
Virtual Machine and API similar to Javacard 3.0	No GUI on the device itself
Accelerometer, temperature and light sensors embedded	Somehow limited cryptographic support
802.15.4 radio communication interface	No absolute location sensor
RSSI radio feedback can sense proximity	Hard to use for a real scenario simulation
Portable and Mobile	It is not a phone

Due to the restrictions of the Sun SPOT platform it was not possible to gather data about the user's activity based on the applications running on the device as it is not a phone nor contains applications similar to the ones used on the mobile phones. Theoretically it would be possible to infer some physical activities based on pattern recognition around the accelerometer. But based on [30] and in experiments we have done with it and the Sun SPOT Telemetry Demo, we could not be able to recognize well activities patterns, as depending on the orientation of the SPOT and the type of physical contact applied to it, the patterns would change. Having stated that, we used the accelerometer to detect a change of state of the user when he starts to move and stops to move. This change of state was employed to optimize the usage of the radio interface as a SPOT would only broadcast sensing packages when it moves.

We used the IEEE 802.15.4 interface for sensing the proximity of two or more SPOTs. We periodically exchanged the Received Signal Strength Indication (RSSI) measurements packets until the connection is broken due to the fact that one of the SPOTs leaves the radio range. Although the radiation power is proportional to the distance, it suffers great variations from interferences. As a result, some tests we have performed signalized more less the same RSSI values for SPOTs in the same room or in rooms separated by walls. Consequently, we decided to use the proximity contextual information only to detect if the SPOTs could sense each other, meaning that their owners were together engaged in a certain interaction further modeled based on their location.

We used the IEEE 802.15.4 packets for sensing the location as well. The location information has been retrieved from location broadcast datagrams emitted by a basestation acting as a location information provider. This was done to emulate the fact that the SIM card would be able to retrieve the location from a mapped Cell-ID, GPS or even from a wireless hotspot. It is in fact feasible to map the hotspots and acquire significant position information, as done by Skyhook or Google Gears Geolocation API. The location packets provide a contextual location that in our scenario was divided in home, outdoor, my office and office's corridor. Nevertheless, the real application should handle more types of contextual locations and possibly be able to convert absolute geographical locations into contextual ones. An illustration of the interaction environment with the 2 free-range SPOTs and the basestation is shown in Figure 1:

We made some tests on fetching attributes linked to an identity managed by an Identity provider, as we personalized the SPOTs with aliases from the social network Last.fm and we used its REST API to retrieve some data. We successfully fetched the favorite artists of the users and their musical compatibility through HTTP requests issued from the SPOTs and routed by a SPOT basestation. However, we opted for not using the attribute values from linked data once most of the work would be related to data mining and crawling, and it would make the trust calculation logic quite complex. Still, we recognize that due to the richness of digital footprints, this kind of information should be taken into account in a future application.

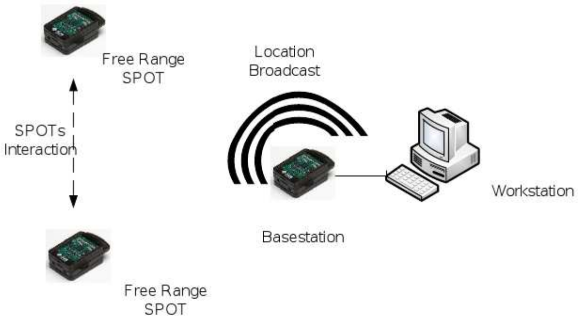

Fig. 1. Communication between the agents in the Sun SPOT implementation.

Being our sensing restrictions set and our goal focused on a proof-of-concept application on the sensing potential, we decided to categorize a trust value for each interaction based on its location and duration. Afterwards, the dispositional trust would be calculated taking into account all the interactions between the users.

For attributing the trust value for each interaction, we first quantify the duration as {passby, short, medium, long} and the location as mentioned before. Based on those values we attribute trust values to three different contextual trusts: professional, private and public as show in the Table 3.

The private context symbolizes relationships on the private level (such as family and friends). The professional context represents relationships related to the person's profession or work. And finally, the public trust context tries to represent people that the user knows, shares some interest but wouldn't necessarily share facts about his personal life. The range of the trust scale used can be seen in Table 4. where each trust value is linked to some meaning, some equivalence that motivated us to quantify it. The 0 is not represented but it means that the agents haven't met. In this model, we do not represent distrust.

In order to assign the value of the contextual dispositional trust between the users at an instant, we put all the values from the previous interactions and their timestamp into a deterministic formula, so that the time degradation of the trust can be represented as well. Instead of using the time elapsed since the interaction as a value measured in time units, we quantify it in three categories recent, past, old. Where recent corresponds to interactions not older than a month; past for the ones in between a month and a year; and old for interactions older than a year. The final formula used is represented by Eq. 1:

$$T_{context} = \frac{0.7}{n'_{recent}} \times \left(\sum_{i=1}^{n'_{recent}} T'_{recent_i} \right) + \frac{0.25}{n'_{past}} \times \left(\sum_{i=1}^{n'_{past}} T'_{past_i} \right)$$

Table 3. Trust Matrix

Location	Duration	Equivalent situation	Prof. Trust	Pub. Trust	Priv. Trust
Home	PASSBY	Someone passes by, no spoken contact	0	1	0
	SHORT	Possibly a home delivery or small talk at the door	0	1	1
	MEDIUM	Someone that is invited to come in	0	2	3
	LARGE	Other people living at home or passing the night	0	5	5
My Office	PASSBY	Someone passes by, no spoken contact	1	0	0
	SHORT	Asking for work-related information, small chat	2	1	0
	MEDIUM	Meeting	4	2	0
	LARGE	Working together in the same room	5	3	2
Offices Corridor	PASSBY	”Cross each other, no spoken contact”	1	0	0
	SHORT	Stopping and chatting in the corridor	1	2	0
	MEDIUM	Activity being performed as having lunch together	3	3	2
	LARGE	NOT DEFINED	-	-	-
Outdoor	PASSBY	Cross each other, no spoken contact	0	0	0
	SHORT	Crossing each other leading to small chat	0	1	0
	MEDIUM	Enrolled in an activity together: cinema, shopping, sport, etc	0	2	1
	LARGE	Enrolled in a daily activity together: travelling, camping, etc	0	4	3

Table 4. Trust Scale

Trust Value	Professional	Private	Public
1	They are from the same company	Somehow privately related	Have met in public contexts
2	They know each other in the work environment	Acquaintance	Know each other from public activities
3	Work in the same department	Close Friend	Share a common interest
5	Work in the same room	Family	Part of a common interest group or organization

$$+ \frac{0.05}{n'_{old}} \times \left(\sum_{i=1}^{n'_{old}} T'_{old_i} \right) \qquad (1)$$

where

$$\begin{aligned} T'_{time_i} &= \{\, T_{time_i} \mid T_{time_i} \neq 0\} \\ n'_{time_i} &= \left| T'_{time_i} \right| \end{aligned}$$

and the time represents the time categories *old*, *past*, *recent*, and T_{time_i} represents each one of the trust values of that time frame category.

4.4 Experiments

The experiments actually started with tests towards recognizing user activity patterns with the accelerometer, inferring the SPOTs proximity through RSSI measures and checking the range of the IEEE 802.15.4 antenna

After we identified the context information we could use, we modeled the trust formula mentioned before and we decided to try it in a small fictional scenario where a relationship between two users is emulated. We created a script describing their relationship, and the interactions that would result of their relationship. Based on that, we decided to individually test the trust model, and then, test the sensing acquisition and input of data in the database.

We considered as the emulation scenario the relationship of two friends that work at the same company but at different departments. Since they work at different departments, they have distinct routines. At work, they mainly meet once a week for having lunch and twice a week while having a small chat at one's office room. Their friendship goes beyond the office routine as once per month they either do an outdoor activity (such as going to the cinema, jogging, etc) or they have dinner at each other's place.

We emulated this routine for the equivalent of two months of the scenario and we noticed that the values of professional trust between the users was in between "knowing each other from work" and "working in the same department", while privately they were close to "acquaintance" and publicly to "know each other". While the professional and private values seemed reasonable, the public one looked somehow underestimated. There was an improvement, although not that significant, of the trust with the insertion of "a common activity outside" and "a dinner at home" between the friends. We also introduced an event corresponding to a trip together for 3 days, and, at this point, the private trust has been increased to a level closer to "close friend", but the public one was still far from "share common interest" level. At last, we simulated a month without contact between the agents, representing a vacation period. After that one month period, the trust events moved to the past category, and their weight in the trust value severely decreased. Nevertheless, they were quickly recovered when the users started again their weekly routine at work together.

4.5 Evaluation

The simple trust inference model shows decent results for the scenario emulated as it converged to reasonable values of professional and private trust between the users and showed both resistance to single events and degradation of the trust values in the case the users lose contact. However this degradation, the event resistance and the accuracy of the values should be reviewed by experts from the sociology and psychology field as they probably will be able to draw more relevant conclusions and propose unbiased adjusts for the logic and quantifications.

Still, we managed to identify a few aspects that could be improved in the model we have used. For example, the mentioned resistance to new inputs is at some point valid as it limits the trust variation from a biased or wrong input. On the other hand it makes the trust value too much dependent on the user's routine. The ideal solution to address this would be to weight the different activities in comparison with the frequency associated with that specific activity, even if this may require much more work characterizing the activities and defining the right weights. In fact the number of events could be a parameter to enhance the trust values, so additional events always contribute positively to the trust value.

We considered modifying some values, especially for the public trust results, on the trust matrix. However, we see that some occasions would assign a trust that does not really exist, i.e. where both users are present at the same place and in the same range but not really establishing trust (as if two people take the same plane for example). For this problem we believe that a further analysis on the activity context could give better inputs to find suitable values for the public trust of the matrix.

Another point that we observed in our experiments is that it would be beneficial to expand the contact from only presence-based to include also other communication formats such as phone calls, e-mails, etc. This would be necessary in order to accurately represent cases such as when the agents separate from each other but still keep contact. It is important to capture the real life interactions, but the virtual ones should be considered as well, possibly with a smaller weight.

In what concerns the platform itself, the Sun SPOTs revealed to be an adequate platform for representing a full featured future SIM. It does lack a real GUI and it lacks the connections with a mobile and a real location sensor. However, its java machine is very powerful and easy to code for it; it is mobile, has a great range of sensors and it is possible to attach other pieces of hardware to it.

We noticed also that the application must define how to consider small interaction interruptions. For example, if two agents are working together in the same office, their interaction would suffer brief interruptions when each one goes separately to the coffee machine or just merely leave the range for a while. The definition of the interval corresponding to the break of the connection should depend on the context of the interaction, the range of the sensing capabilities of the agents and the model itself.

5 Conclusions and Future Work

This work presented an approach towards using the new advanced sensing and communicating capabilities of the SIM card in order to support trust applications and specifically trust relations in social networks. We established functionalities of future SIM cards such as motion and location detection by emulating them on the Sun SPOTs.

Several context sensing possibilities were identified for modeling the trust relation between two entities based on hard evidences sensed during their interactions. Moreover, we used some of those contexts in a simple model to prove this seamless trust builder concept. We emulated a routine of co-workers spanning an equivalent of two months, resulting in values of professional trust between the users as an intermediate of "knowing each other from work" and "working in the same department". Their private trust value was close to "acquaintance" and their public trust value "know each other".

The experiment has shown that attributing dispositional trust values between users based on sensing the context between their interactions is feasible. First results for this sensor-supported trust model look promising. In order to accurately represent the dispositional trust between users, it is necessary to further adjust the input values for our trust model by characterization and quantization of the inputs and outputs with experts of cognitive sciences. Moreover it is advisable to deploy a broader experiment with several distinct cases and preferably with real people.

References

[1] Breslin, J., Decker, S.: The future of social networks on the internet: The need for semantics. IEEE Internet Computing **11**(6) (2007) 86–90

[2] Beattie, R.: Linking out after two years of linked in. Web site: http://www.russellbeattie.com/notebook/1008411.html [Last accessed: 31/05/09] (2005)

[3] Ann Golbeck, J.: Computing and applying trust in web-based social networks. PhD thesis, University of Maryland, College Park (2005)

[4] Renaudin, M., Bouesse, F., Proust, P., Tual, J.P., Sourgen, L., Germain, F.: High security smartcards. In: DATE '04: Proceedings of the conference on Design, automation and test in Europe, Washington, DC, USA, IEEE Computer Society (2004) 10228

[5] Markantonakis, C., Mayes, K., Tunstall, M., Sauveron, D., Piper, F.: Smart card security. In Nedjah, N., Abraham, A., de Macedo Mourelle, L., eds.: Computational Intelligence in Information Assurance and Security. Volume 57 of Studies in Computational Intelligence. Springer (2007) 201–233

[6] GlobalPlatform Inc.: GlobalPlatform, Card Specification Version 2.2. (March 2006)

[7] ETSI: ETSI TS 102 483: Smart cards; UICC-Terminal interface; Internet Protocol connectivity between UICC and terminal V8.1.0. (April 2009)

[8] Eisl, F.: Smart card security services for an open application environment used in mobile phones (June 2004)

[9] OMA: Smart Card Web Service Standard Version 1.1. (2009)

[10] ETSI: ETSI TS 102 613: Smart Cards;UICC - Contactless Front-end (CLF) Interface;Part 1: Physical and data link layer characteristics V7.5.0. (April 2009)

[11] ETSI: ETSI TS 102 622: Smart cards; Smart Cards;UICC - Contactless Front-end (CLF) Interface;Host Controller Interface (HCI) V7.4.0. (April 2009)

[12] PRNewswire.com: Oberthur technologies announces simsense - the first motion detection sim card. http://news.prnewswire.com/ViewContent.aspx?ACCT=109&STORY=/www/story/02-16-2009/0004972701&EDATE= [Last accessed: 31/05/09] (2009)

[13] Cellular-news: Sagem to embed gps receiver into sim cards. http://www.cellular-news.com/story/34691.php [Last accessed: 31/05/09] (2008)

[14] Brede, S.: ETSI Workshop presentation 4-5 june 2008 A couple of M2M activities: WLANSIM a wireless IP networked UICC. Telenor R & I. (2008)

[15] Turolla, M., Alessio, E.: presentation ZSIM enabling innovative services to improve quality of life. Telecom Italia Innovation & Engineering. (2006)

[16] 3GPP: ETSI TR 133 980: Digital cellular telecommunications system (Phase 2+);Universal Mobile Telecommunications System (UMTS);Liberty Alliance and 3GPP security interworking;Interworking of Liberty Alliance Identity Federation Framework (ID-FF), Identity Web Services Framework (ID-WSF) and Generic Authentication Architecture (GAA) V7.6.0. (October 2007)

[17] Sun Microsystems, Inc.: Runtime Environment Specification: Java Card Platform, Version 3.0, Connected Edition. (March 2008)

[18] Johannessen, T.: Identity management in general and with attention to mobile gsm-based systems. Telektronikk (2007) 31–51

[19] GSM Association.: Identity Management Framework Document V1.1. (2008)

[20] Stutzman, F.: An evaluation of identity-sharing behavior in social network communities. In: Journal of the International Digital Media and Arts Association. (2006)

[21] Fogel, J., Nehmad, E.: Internet social network communities: Risk taking, trust, and privacy concerns. Computers in Human Behavior **25**(1) (January 2009) 153–160

[22] Korpipää, P., Mäntyjärvi, J., Kela, J., Keränen, H., Malm, E.J.: Managing context information in mobile devices. Pervasive Computing, IEEE **2**(3) (2003) 42–51

[23] Schmidt, A., Laerhoven, K.V.: How to build smart appliances. IEEE Personal Communications **8** (2001) 66–71

[24] Hristova, A.: Conceptualization and design of a context-aware platform for user-centric applications (June 2008)

[25] Mayes, K.E., Markantonakis, K.: On the potential of high density smart cards. Information Security Technical Report **11**(3) (2006) 147–153

[26] Katz, Y., Golbeck, J.: Using social network-based trust for default reasoning on the web

[27] Taherian, M., Amini, M., Jalili, R.: Trust inference in web-based social networks using resistive networks. In: ICIW '08: Proceedings of the 2008 Third International Conference on Internet and Web Applications and Services, Washington, DC, USA, IEEE Computer Society (2008) 233–238

[28] Bražinskas, R.: Towards context awareness using mobile sensors (2008)

[29] Chang, E., Dillon, T., Hussain, F.: Trust and reputation for service-oriented environments : technologies for building business intelligence and consumer confidence, Wiley (2006)

[30] Karantonis, D.M., Narayanan, M.R., Mathie, M., Lovell, N.H., Celler, B.G.: Implementation of a real-time human movement classifier using a triaxial accelerometer for ambulatory monitoring. Information Technology in Biomedicine, IEEE Transactions on **10**(1) (2006) 156–167

[31] AlNemr, R., Meinel, C.: Getting more from reputation systems: A context-aware reputation framework based on trust centers and agent lists. International Multi-Conference on Computing in the Global Information Technology (2008) 137–142