[**Publication 3**] Zheng Yan and Piotr Cofta, "Methodology to Bridge Different Domains of Trust in Mobile Communications", In *Proceedings of the 1st International Conference on Trust Management (iTrust 2003)*, LNCS Vol. 2692/2003, pp. 211-224, Greece, May 2003.

http://www.springerlink.com/openurl.asp?genre=article&issn=1611-3349&volume=2692&spage=211

Methodology to Bridge Different Domains of Trust in Mobile Communications

Zheng Yan[1], Piotr Cofta[2]

[1] Nokia Research Center, Nokia Group, Helsinki, Finland
[2] E-Business & Security – Mobile Software, Nokia Group, Finland

{zheng.z.yan, piotr.cofta}@nokia.com

Abstract. Trust is playing an important role in communications and transactions. Based on different reasons of trust, different trusted domains, possibly disjoint, are formed in mobile communications, preventing complete systems from working properly. What is lacked therein is a bridge that can link domains, across trust gaps to establish a complete trusted mobile communication system. In this paper, the authors propose a generic method to analyze and model a mobile communication system into a number of trusted domains. In order to overcome the trust gaps among the originally disjoint domains, the authors further propose three approaches to bridge different domains and demonstrate the use of mobile Personal Trusted Devices, such as mobile handsets to act as the said bridge.

1 Introduction

Trust is an important aspect in the design and analysis of secure distributed systems [1]. Recently, trust modeling is paid more and more attention in mobile communications.

Actually, trust is such a subjective and dynamic concept that different entities can hold different opinions on it even while facing the same situation [2]. Based on different trust perception, different trusted domains can be formed also in the area of mobile communications. For example, a trusted domain that contains a security element (such as a smart card) and its issuer is formed if the issuer trusts the security element due to its tamper resistance. A trusted domain containing a personal mobile device (e.g. a mobile phone) and its holder can be constructed if the device holder trusts the device because its brand has a good reputation. An operator trusts its SIM (Subscriber Identity Module) card due to the embedded cryptography inside. A SIM card trusts the phone it is inserted into because otherwise it has no chances to operate.

In today's mobile communications, we can find many cases in which a system is actually formed by a number of the trusted domains and the communications and transactions are actually conducted among and across those domains. Significant problem may arise from the fact that different domains must cooperate in order to provide a complete service even though they may not share the same concept of trust. Specifically, security problems may be caused by the deficiency of trust among domains. This deficiency is likely one of the major barriers that prevents the proliferation of the mobile communications and transactions. The deficiency of trust is visible as gaps between the trusted domains established by different entities. For example, the proper arrangement for secure interaction between a smart card that belongs to a trusted domain of the card issuer and a terminal based application that belongs to a trusted domain of an application developer has been causing a lot of problems for a very long time. As another example, identification of autonomous and potentially malicious nodes in an ad-hoc network is both a security and a trust challenges that have raised many arguments.

There are several methods to bridge the trust gap, e.g. legal, contractual, and risk management based solutions. The authors believe that technology is one of the most important methods. In this paper, a technical method to bridge the trust gap is provided. The authors propose a methodology to analyze and bridge the trust domains and then study the use of mobile Personal Trusted Device to work as a trusted bridge for certain use cases derived from the mobile communications and transactions area.

The rest of the paper is organized as follows. Section two provides an overview of related trust schemes in literature. Section three introduces necessary definitions while the next section proposes the method to bridge the trusted domains in the mobile communications. In section five, the applicability of the proposed method is illustrated by applying it to some realistic examples. Finally, conclusions are provided in the last section.

2 Related Work

Current academic work related to the trust covers wide area of interest ranging from such aspects as perception of trust [4, 5], problem analysis of current secure systems [11, 12], trust modeling [7, 8, 9, 10], to trust quantification and specification in digital systems [3, 6].

The concept of trust is defined in various ways in the literature [2, 4, 5, 11, 14, 16]. It is widely understood that the trust itself is a comprehensive concept, which is hard to narrow down. The trust is subjective because the level of trust considered sufficient is different for each entity. The trust is also partly objective as it is affected by those factors that we cannot monitor.

Several papers discuss the role and models of trust applied to electronic communication. For example, a trust model for a secure multi-agent marketplace in [13] is based on a concentric sphere structure. The core of this model is the physical security. A security infrastructure is located in middle sphere: an internal and an external security infrastructure. In outer sphere, this model uses complex aspects of the trust such as fairness, reliability, reputation and loyalty to provide a complete model of basic trust for marketplaces. Unfortunately, this work did not illustrate how to apply the model into real systems.

Another interesting work in [8] provides a generic model of transaction trust for electronic commerce. This model is based on separating the mostly subjective party trust and mostly objective control trust. In the authors' opinion, party trust + control trust = transaction trust. If the level of the transaction trust is not sufficient for the transaction then the party trust should be possibly complemented by the control trust in order to reach the required level. This work focuses on the Internet based transactions. It did not consider the scenarios of the mobile communications.

Further, work in [14] gears towards trust management and describes an authentication trust model, as well as a schema for managing access control in a multi-agent system. The trust model and trust management framework proposed can take advantages of a number of trust management schemas, such as SPKI (Simple Public Key Infrastructure), RBAC (Role Based Access Control) and Kerberos, for delegation of authorizations. Similarly, in [10], a model for trust is proposed based on distributed recommendation. These work do not examine their applicability for the mobile communications. In addition, they cannot solve the trust gap problem.

As it can be seen from the short discussion above, none of the existing work tried to address trust in the mobile communications that have its own salient characteristics, and where mobile devices play a very important role by supporting communication mobility and flexibility. Further, no work considered or dealt with the trust gap problem that can be found. A new methodology to bridge different domains of trust is therefore needed to overcome these issues.

3 Definitions

Due to multiplicity of meanings associated with the word 'trust' and its derivatives, it is essential to establish certain set of definitions that can be used throughout the paper.

The working definition of trust used in this paper bases on [16] where the trust is defined as the confidence of an entity on another entity based on the expectation that the other entity will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other entity. Note that the methodology presented in this paper is not sensitive to the exact definition of trust.

3.1 Trusted domain

The trusted domains are not the entirely new concept in the literature, but so far, the authors have not found a concrete definition in available references. Herein, the following definition of the trusted domain is used throughout the paper.

Definition 1. Trusted Domain

> A trusted domain is a set of domain entities (e.g. service providers), defining statements and domain components (e.g. devices) such that all domain entities share certain defining statements regarding their trust definition for specified purpose, and all domain components adhere to such trust definition and implement the statements. The defining statement identifies requirements of the domain entities that must be fulfilled by the domain components to be trusted.

In Fig.1, an example of three trusted domains is presented. Domain *D1* consists of an entity *A* and two statements *s1* and *s2*. The statement *s1* does not define any existing component (i.e. there are no components that fulfill the statement) while the statement *s2* defines two components *a* and *b*. Domain *D2* contains entity *B* and two statements. The statement *s1* (identical with one of the statements from the domain *D1*) defines component *c* while statement *s3* defines component *d*. Finally domain *D3* has two entities: *C* and *D* with two statements. Statement *s4* defines two components *d* and *e*, in which the former is shared with the domain *D2*. Statement *s5* defines two components *e* and *f*, in which the former is also defined by the statement *s4*. Note that the component *d* fulfills both the statement *s3* and *s4*, so that the *D2* and *D3* are naturally bridged by the component *d*.

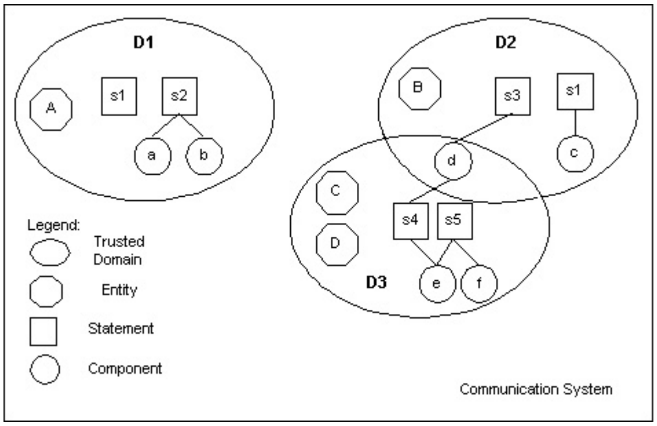

Fig. 1. An example of three trusted domains in a communication system

In other words, a trusted domain is established whenever some entity or entities (such as a user, an operator or a service provider) trusts some components for the specific purpose, regardless of the reasons for the trust that can be both subjective and objective, either rational or irrational. In this paper, special interest is placed in the domains where their components are hardware or software components in a digital system.

For example, the mobile operator creates its own domain of trust that includes, among others, SIM cards. The operator may trust the SIM cards that are fitted in mobile phones for the purpose of user authentication. The reason the operator trusts its SIM cards is likely to be rational and may come from the understanding of physical and cryptographic properties of the card as well as the quality of personalization process. The user defines his/her own domain of trust. The user may also trust the SIM card for the purpose of billing relationship due to effective user authentication. However, this trust may be less rational but rather driven by the popularity of technology or the visibility of the operator's brand. In this example the operator forms its own domain that is built on its understanding of trust while the user forms another domain on the basis of the user's defining statement. The SIM cards exist in both domains, thus enabling the mobile communication.

In another example, the user attempts to roam in another country where no roaming agreement exists between the user's home operator and current operator. Even though the configuration is technically identical, the current operator does not trust the user's SIM. Effectively, the user's SIM is out of the operator's trust domain and the user cannot use the mobile network.

3.2 Trusted bridge

Based on the above definition and examples of the trusted domain, we can see that the full trust is retained inside the trusted domain while the trust may be missing among the domains. This may cause the trust gap in places where the trusted domains do not overlap.

For the success of the mobile communication systems, all the trusted domains that are essential for the complete system must intersect, i.e. there must be at least one component (or a chain of them) that is trusted by the entities communicating with each other. If it is not the case, a bridging solution should be identified and on that basis the bridging component must be created. Such trusted bridge can be as simple as the component that is trusted by both domains, or complex, with its own respective entities, statements and components that can bridge the disjoint trusted domains.

Definition 2. Trusted Bridge

> A trusted bridge is a component or a set of components that is/are trusted by more than one domain. Therefore such component(s) can work as a bridge to establish the trust among those domains. Note that if any of the bridged domains contain more than one statement, it is sufficient for the trusted bridge to implement one of those statements for each of the domains it is bridging.

In Fig.1, the domains *D1* and *D2* are disjoint and no trust can be readily established by any technical means, while the domains *D2* and *D3* intersect so that the component *d* can be used to establish the trust between them.

As illustrated by the previous example, the SIM card operating in the home network acts as a bridge between the operator's domain and the user's domain. If, for example, the operator extends its domain to cover some digital content merchants, they can immediately benefit from the existing trusted bridge.

3.3 Personal trusted device

Most of use cases in the section five explore the applicability of a Personal Trusted Device (PTD) to bridge the trust gap. Certain references to the concept of PTD can be found in [16]. Due to the fact that there is no formal definition of the PTD, the working definition is provided below.

Definition 3. Personal Trusted Device (PTD)

> PTD is a platform device that accepts multiple technologies with special focus on mobile communications and is personal to its user.

Further it will be demonstrated that by exploring the above properties the PTD can become a trusted bridge for the multiplicity of services thus acquiring desired trust property that has been intentionally removed from the original definition of the PTD.

The mobile phone acting as the PTD plays an important role in the mobile communications. It has hardware support for the trust, such as a slot for the smart card. Tamper-resistant device like the smart cart inside the mobile phone offers high level of trust through security. Most of the mobile phones have a SIM (Subscriber Identity Module) card, trusted by the mobile network operator who can audit the phone's network activities. In addition, the mobile phone can hold a WIM (WAP Identity Module) card (either as a separate card or as an application located at the SIM card) for generating digital signatures that can realize non-repudiation. With its inherent characteristics of mobility, portability and security, the mobile phone is very flexible in approaching any other devices to realize communications regardless of time and location. The PTD implemented by the mobile phone is therefore potentially the best device that can link the user, the operator and the service providers, acting as a bridge for several mobile services.

4. Methodology

In this section, the authors introduce a new methodology into the area of mobile communications. This methodology helps to analyze the trust inside any mobile communication system by modeling the system into a number of trusted domains formed by different entities. In order to solve the issue of trust gaps, the authors further propose three approaches to bridge the disjoint domains.

In any mobile communication and transaction system, we can always specify the system as a number of trusted domains. The communications and transactions are actually conducted among those domains. Inside each trusted domain, the domain entities trust the domain components according to their defining statements, for whatever reasons they find appropriate. Among the trusted domains, it is expected that the trust must be usually created and constructed logically and rationally. The authors propose the methodology to analyze the trust domains and to create the trusted bridge, effectively enabling the domains to form a complete solution. The proposed methodology is summarized as follows.

1. Model the mobile communication system by separating it into a number of trusted domains formed by different entities.
2. Analyze each domain in order to extract the defining statements and list existing domain components. The resulting graph may resemble Fig.1.
3. For each pair of disjoint domains that must trust each other for the purpose of a given service, seek bridging solution that can satisfy both domains (see the discussion below).

4. Form the trusted bridge by finding or creating the suitable component (or components), or by establishing bridging domains, depending on needs (see the discussion below).

There are several approaches to identify the bridging solution and to introduce the trusted bridge, depending on the defining statements within the trusted domains as well as on non-technical limitations. Following is a short list of those. Throughout the discussion, the domains *D1* and *D2* from the definition of the trusted bridge (as shown in Fig. 1) will be used to illustrate concepts.

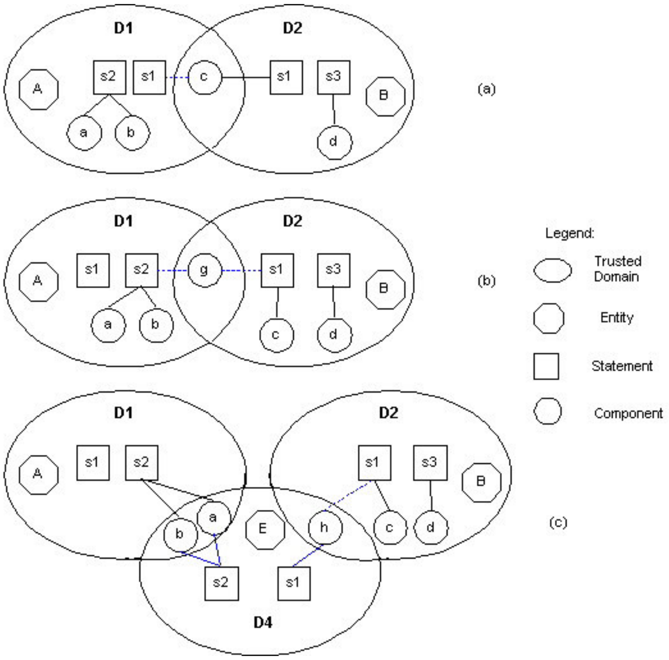

Fig. 2. Methods of bridging trusted domains

a. Use existing component (Fig.2.a.)

The analysis itself may lead to the discovery that there is already an existing component that may be trusted by more than one domain. Even though such solution may seem trivial, it is the trust-based analysis itself that is frequently needed. For example (Fig.2.a), as the domains *D1* and *D2* share the same defining statement *s1*, it is sufficient to verify that the component *c* (currently within the domain *D2*) that fulfills the statement *s1* is accepted also by *D1*.

b. Create new component (Fig.2.b.)

If the bridging component does not exist it is possible to create it. Some components may conform to only one statement so that they require the identical statement in both domains. Some components may conform to more than one statement so that they can be used to bridge the domains with different statements. Note that the meaning of the identity of defining statements requires further discussion that goes beyond the scope of this paper.

The use of multi-statement component has been already demonstrated at the intersection of the domains *D2* and *D3*. Such solution is also viable for the domains *D1* and *D2*, e.g. in a form of a component *g* that conforms to both the statements *s2* and *s1*, as shown in Fig.2.b.

c. Create separate domain (Fig.2.c.)

If there is no potential component that may satisfy the domains (e.g. the statements are significantly different), the solution may be to create a separate domain such that its domain components fulfill statements from both disjoint domains. Such domain may share existing or new components with all the domains it is bridging. The authors call the created domain as bridging domain.

For example, domain *D4* can be introduced to bridge disjoint domains *D1* and *D2*. Domain *D4* consists of the entity *E* and three components: the existing components *a* and *b* that conform to the statement *s2* and is trusted also by the *D1* and a new component *h* that conforms to the statement *s1* and is trusted also by the *D2*.

If necessary, the creation of the new domain can be repeated to form the chain of domains until the bridging is complete, i.e. until there is at least one chain of domains that links all the domains that were originally disjoint. Obviously, it is possible to get multiple solutions to bridge trusted domains. It depends on further analysis and concrete systems requirements to decide which one is the best.

The authors further propose the PTD that could be implemented by a mobile phone to work as the trusted bridge for the purpose of the mobile communications. It is obvious that the PTD which is the platform that is possibly trusted by both the user and the operator can be deployed as a component that satisfies almost all domain entities in the mobile communication systems.

It is significant that this methodology can also be applied into any system analysis and design. It provides a special approach on security analysis from the trust point of view. Based on the analysis, it is clear to know what is lacked and therefore needed in the system. It will be also potentially easier to find the proper component with appropriate technologies to bridge the trust gap that otherwise may cause the security problems. Therefore, this methodology helps us to set up a secure and trusted system and aids us to seek new business opportunities, e.g. via seeking the proper trusted bridges to find new products or novel functions.

5 Applicability

In this section, the authors will illustrate how to apply the proposed methodology into different scenarios and expound how the PTD can work as the trusted bridge to overlay the trust gaps among the trusted domains in the mobile communications.

Note that this chapter does not aim at providing complete solutions but merely to illustrate the methodology. The outcome, even though it actually conforms to historical information, should not be considered the only or the perfect solution for analyzed cases.

5.1 Mobile trust interaction (inside mobile terminal)

This case demonstrates the use of approach (a) - discovery of the existing component that can be used to bridge the domains.

Looking inside today's mobile terminals, we are facing the trust gap problem. The issue of interaction between a security element (SE) (such as a smart card, e.g. SIM) and terminal based applications has been discussed for a very long time. The lack of general solution has been slowing the development of possible exciting applications, especially in mobile commerce. The problem lies in the trust deficiency between the SE and the terminal-executed applications, such as Java MIDlets, Symbian applications and web pages.

The recent development of signed applications (e.g. Symbian application, OMA (Open Mobile Alliance) signed content and MIDP (Mobile Information Device Profile) 2.0 environment) has brought new interesting aspect into such scenario.

The common perception across the industry is as follows. The terminal application and the SE come from different trusted domains established by different entities. The signed application (e.g. a MIDlet) is trusted by its developer, which is expressed by the fact that the developer signs the application. The smart card, a SE, is trusted by the card developer. Finally, the user of mobile device basically trusts what he/she sees at the device.

All the three trusted domains enter the terminal and meet there when the application attempts to access the SE, which is usually combined with certain user interaction. Those trust domains should overlap somewhere, where the interaction between the application, the SE and the user are in place. However, one problem is that they do not overlap because there is no method to introduce the sufficient trust among those domains of those entities.

Implementing the proposed methodology, the following observations can be made, leading to the complete picture as shown in Fig.3.

1. The application developer trusts his application (*s1*) as it is him who developed it. Further, the application developer trusts (*s2*) the signing process usually derived from the PKI (Public Key Infrastructure) technology and the implementation of delivery and verification mechanisms for installing and running the application on the mobile terminal.
2. The card developer trusts the card due to its tamper-resistance (*s3*) while he/she does not necessarily trust any particular cryptographic system. The card developer

trusts also the same terminal (*s4*) regarding its ability to convey correctly messages between the application and the card as well as regarding the correct handling of the user interaction.

3. The user trusts in what he/she sees on the terminal (*s5*). This trust is not based on any particular technology, but on the combination of several psychological factors.

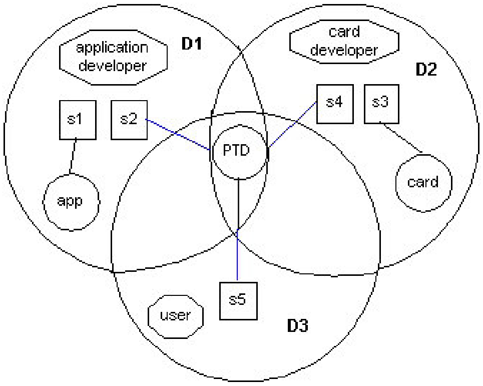

Fig. 3. Mobile trust interaction inside mobile terminal

Note that the methodology has immediately discovered three hidden statements, all applying to the terminal. Even though the three trusted domains are driven by different statements, all of them share the same component: the terminal that can be the mobile PTD. Therefore the PTD can potentially serve as the bridge to overlay the trust gap, e.g. by defining the access control mechanisms so that only certified applications can access designated objects on the card via the interaction with the user.

5.2 Mobile services

The case of mobile services is used here to demonstrate the approach (b) - identifying the new common component.

The term 'mobile services' can be vaguely defined as services that are provided to mobile users via the mobile terminals, e.g. messaging, browsing, and shopping. Specifically, the mobile terminals such as the mobile phones and mobile PDAs (Personal Digital Assistants) are considered to be the key element of mobile services. The key problem of mobile services seems to be the identification of the user for the purpose of service delivery and billing.

As the mobile phone has already had the trust relationship (*s1*) with its operator through the existence of SIM and relevant authentication methods, the analysis leads to the outcome depicted in Fig.4 (solid lines and plain text only). Naturally the users trust their terminals (*s2*) mostly due to the good reputation of terminal manufacturers.

The service provider stays out of the usual trust relationship due to the fact that no component in possession of the user falls into its domain *D2*.

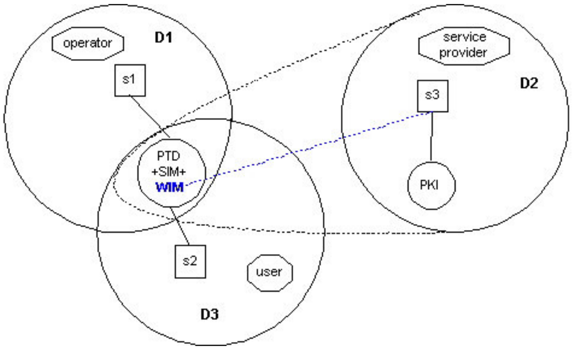

Fig. 4. Trust interaction in mobile services

The service providers have been creative to overcome the trust gap, e.g. by going with the operators and re-using the existing authentication and billing infrastructure. By doing this, the service providers effectively moved themselves into the operator's domain. Alternatively they established the independent component with the users through the sign-in process (e.g. a password), even though it has led to several inconveniences for the user.

An analysis revealed that the service provides who are not willing to move into the operator's domain are expressing significant trust in PKI technologies (*s3*). However, the use of such technologies requires an independent identification element in the terminal. Such element can be established in a form of a second card, WIM, sharing the same terminal with the SIM, as depicted on Fig.4 (dotted lines and bold text). The re-designed mobile terminal, essentially realized by the PTD, can therefore bridge the trust gap.

This scenario also demonstrates that not all solutions that are technologically sound may easily enter market. Despite of the existence of dual chip phones they are not the most popular solution for the mobile services. Alternative solutions like SWIM (Subscriber and WAP Identity Module) where SIM and WIM reside in the same card or 'white WIM' where the blank smart card owned by the user is issued to the phone are also not popular. The complete analysis of such solutions from the trust perspective that may deliver interesting observations is unfortunately beyond the scope of this paper.

5.3 Mobile Ad Hoc Networks (MANET)

This use case demonstrates the method (c) - introduction of new domains to bridge the disjoint domains.

Ad hoc networks are a new paradigm of networks offering unrestricted mobility without any underlying infrastructure. The mobile ad hoc network (MANET) is a collection of autonomous nodes or terminals that communicate with each other over relatively bandwidth-constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized. Thus all network activities including discovery of the topology and delivery of messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into the mobile nodes. The MANETs are generally more prone to physical security threats. The possibility of eavesdropping, spoofing, denial-of-service, and impersonation attacks increases. Significant applications of the MANETs include establishing survivable, efficient, dynamic communications for emergency/rescue operations, disaster relief efforts, and military networks that cannot rely on centralized and organized connectivity.

The problem studied here is the identification of the nodes constructed by ad hoc terminals. It is one of the most important problems of the ad hoc network, which effectively prevents such networks from wide deployment.

Applying the proposed methodology one can produce the graph as depicted in Fig.5 (solid lines and plain text only). Each node is effectively an island for itself, driven by its own statement. For example, if the node is in the possession of the user (user 1 in domain *D1*), statement (*s1*) may base on the trust on reputable brand or shared password. The nodes that reside in a corporate building attached to certain devices (domain *D2*), may be trusted by corporation (user 2) because of its semi-permanent supervised location (*s2*).

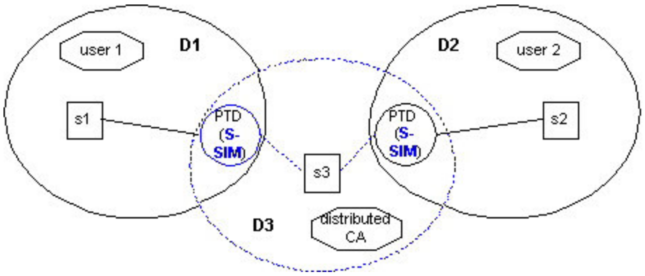

Fig. 5. Trust interaction of identification in ad hoc networks

As the nodes cannot trust each other regarding their identities, they cannot establish any meaningful service. Further, the methodology demonstrates that in the general case there is nothing in common between two nodes except for their communication capabilities. In such case the introduction of additional domain seems to solve the problem.

The authors propose to introduce the bridging domain created by a distributed CA introduced in [17] that trusts its authentication system (*s3*). The CA converts nodes into multi-statement-supported devices by adding an authentication component that can be a SIM signed by the distributed CA (called here S-SIM), as illustrated in Fig.5

(dotted lines and bold text). A centralized CA (e.g. the operator) can also work for the initialization of the ad hoc network via issuing the authentication component (e.g. S-SIM) and distributing partial secrets to the nodes. The signature signed by over a threshold number of nodes can be treated as valid. Those nodes may cooperate to behave as a distributed CA in the future, because the centralized CA most possibly may lose contact with the nodes after the network starts running. In that case, the distributed CA acted by the nodes themselves will start to play the role of CA as an essential backup.

Another challenge in the ad hoc network is that every node has to depend on other nodes to delivery data package, including routing information. At the same time every node must not readily trust any other nodes because they are more easily to be captured, compromised and hijacked. Further, attacks raised from malicious nodes inside the network are much harder to detect as they hold the correct identities.

As stated above, this use case is the illustration of the methodology, not the solution of the security problem in the ad hoc networks. Other solutions that can be derived from the same methodology can be considered as well. Specifically, trust evaluation may be of some interest, as shortly described below.

Instead of aiming at perfect identity and full trust, the node may live with partial trust because the identity can be spoofed. Based on the work in [1, 4], the trust can be evaluated and processed digitally by quantifying its variables such as transaction cost, transaction history, recommendations and reputation data. The authors hold opinion that the above trust evaluation should be conducted digitally ahead of any communication and the evaluation result should be considered for better security decision. This mechanism should be embedded into every ad hoc terminal.

Note that the node terminal fitted with the identification mechanism (such as the S-SIM) and the trust evaluation mechanism can be realized by the PTD that behaves as the trusted bridge in the ad hoc networks.

6 Conclusions

In this paper, the authors introduced a methodology to bridge the domains of trust in mobile communications. It has been proposed that any system analysis and design could include modeling the system as composed of different trusted domains that may reflect various reasons for the trust. Inside the domain, the trust relationship has been established, while among domains the trust is deficient. Thus in this way, it is easier to identify the trust and security problems hidden inside the system. In order to bridge the trust gaps, the authors further proposed three approaches and illustrate their applicability through the real industry cases.

Based on this study, it has been found that the PTD, such as the mobile phone, plays an important role in the mobile communications and transactions. It is in a unique position contributing to the system trust and security by overlaying the trust gaps among various the trusted domains with corresponding functionalities. The special role of the PTD to establish the trust claims that it fully deserves its name as the Personal Trusted Device. The applicability study further proves that the methodology is generic and helpful in the analysis and design of various mobile systems. The authors believe that it can also be applied into other areas to solve similar issues.

References

1. Diamadi, Z. Fischer, M.J.: A simple game for the study of trust in distributed systems. International Software Engineering Symposium 2001 (ISES'01), Wuhan University Journal of Natural Sciences Conference (March 2001).
2. Diego Gambetta.: Can We Trust Trust?. In, Trust: Making and breaking Cooperative Relations, Gambetta, D (ed.) Basil Blackwell. Oxford, (1990).
3. Daniel W. Manchala: Xerox Research and Technology. E-Commerce Trust Metrics and Models. IEEE Internet Computing, vol.4, no.2 p.36-44 (2000).
4. McKnight, D. Harrison, Chervany Norman L.: The meanings of Trust. In <http://www.misrc.umn.edu/wpaper/wp96-04.htm>
5. McKnight, D. Harrison, Chervany Norman L.: What is Trust? A Conceptual Analysis and An Interdisciplinary Model. In Proceedings of the 2000 Americas Conference on Information Systems (AMCI2000). AIS, Long Beach, CA (August 2000).
6. Mui Lik, Mohtashemi Mojdeh, Halberstadt Ari: A Computational Model of Trust and Reputation. In Proc. Of the 35th Annual Hawaii International Conference on System sciences, 7-10 (Jan. 2002), Big Island, HI, USA
7. Warne, D., Holland, C.P.: Exploring trust in flexible working using a new model. BT Technology Journal, vol.17, no.1, p.111-119. (Jan 1999).
8. Yao-Hua Tan. Thoen, W.: Toward a generic model of trust for electronic commerce. International Journal of Electronic Commerce vol.5, no.2, p.61-74, 1998.
9. Egger Florian N.: Towards a Model of Trust for E-Commerce System Design. In Proc. Of the CHI2000 Workshop: Designing Interactive Systems for 1-to-1 E-commerce.
10. Abdul-Rahman Alfarez, Halles Stephen: A Distributed Trust Model. In Proc. Of New Security Paradigms Workshop, ACM, New York, NY, USA (1998).
11. Gerck Ed. Overview of Certification System: X.509, PKIX, CA, PGP & SKIP. In <http://www.thebell.net/papers/certover.pdf>
12. Perlman, R.: An overview of PKI trust models. IEEE Network, vol.13, no.6 p.38-43.
13. Robles, S., Borrell, J., Bigham, J., Tokarchuk, L., Cuthbert, L.: Design of a trust model for a secure multi-agent marketplace, Fifth International Conference on Autonomous Agents, Montreal, Canada (05.2001).
14. Wu Wen, Mizoguchi, F.: An authorization-based trust model for multiagent systems, Applied Artificial Intelligence vol.14, no.9 p.909-925, 2000.
15. Mayer, R.C., Davis, J.H., Schoorman, F.D.: An Integrative Model of Organizational Trust, Academy of Management Review, Vol. 20, No 3, pp. 709-734 (1995).
16. MeT Personal Trusted Device Definition (2001) <http://www.mobiletransaction.org/pdf/R11/MeT-PTD-Def-R11.pdf>
17. L. Zhou, Z. J. Haas: Securing Ad Hoc Networks. IEEE Network, 13(6): 24-30 (Nov/Dec 1999).