[**Publication 2**] Zheng Yan, “A Conceptual Architecture of a Trusted Mobile Environment”, In *Proceedings of IEEE 2nd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU06)*, held in conjunction with IEEE International Conference on Pervasive Services 2006, pp. 75-81, France, June 2006.

A Conceptual Architecture of a Trusted Mobile Environment

Zheng Yan
Nokia Research Center, Helsinki, Finland
zheng.z.yan@nokia.com

Abstract

Trust is crucial in mobile communications. How to establish a trusted mobile environment is becoming more and more important for mobile device venders, mobile service providers and mobile networking operators. This paper presents a conceptual architecture towards establishing a trusted mobile environment. The contribution of this paper is a) specifying the architecture of a trusted mobile environment; b) by developing the conceptual architecture, explaining key motivations behind the location of every element in the architecture; and c) evaluating the architecture by applying it into a mobile peer-to-peer system.

1. Introduction

With the rapid growth of mobile communication technologies, it is convenient for people to use their mobile devices to do various things. People more and more depend on mobile communications in their social life. Life goes mobile.

Mobile commerce and mobile services hold the yet unfulfilled promise to revolutionize the way we conduct our personal, organizational and public business. Some attribute the problem to the lack of a mobile platform that all the players may trust enough. Nowadays, it is very hard to build up a long-term trust relationship among manufactures, service/application providers and mobile users. This could be the main reason that retards the further development of mobile applications and services.

On the other hand, new mobile networking is raising with the fast development of mobile ad hoc networks (MANET) and local wireless communication technology. It is more convenient for mobile users to communicate in their proximity to exchange digital information in various circumstances. However, the special characteristics of the new mobile networking paradigms introduce additional challenges on security [1].

More interesting and strange phenomena is current mobile systems are designed based on the assumptions that a) the user trusts his/her device totally; or b) the user has to trust a service provider; or c) the user has no choice except using some manufacture's device in order to deploy some mobile applications or mobile services. Generally, the systems are not designed considering the users' trust preferences, thus the systems produced are hard to be finally accepted by the end users.

All of the above problems influence the further development of mobile applications and services targeting at different areas, such as mobile enterprise, mobile networking and mobile computing. The key reason is we lack a trusted mobile environment that could support trusted mobile applications and services in the above areas. This paper introduces a conceptual architecture in order to help establishing a trusted mobile environment. Based on this architecture, it could be easier to identify motivations behind each element inside. It also helps solving trust related problems via applying this architecture into real application scenarios.

The rest of the paper is organized as follows. Section 2 introduces the conceptual architecture. Based on the specification of the conceptual architecture, section 3 presents the key motivations for establishing the trusted mobile environment. Section 4 applies this architecture into a mobile peer-to-peer system in order to illustrate this architecture's expressiveness and advantages. The conclusions are given in the last section.

2. A Conceptual Architecture

There is a large range of existing work on trust in information technology. Current academic work related to trust covers a wide area of interest ranging from such aspects as perception of trust [2], problem analysis of current secure systems [3], trust management and modeling [4-6], trusted computing [7-8], to trust quantification and specification in digital systems [9, 10]. But there are still many issues

Proceedings of the Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU'06)
0-7695-2549-0/06 $20.00 © 2006 IEEE

regarding trust that are worth further study in order to support further success of mobile computing, communications and services.

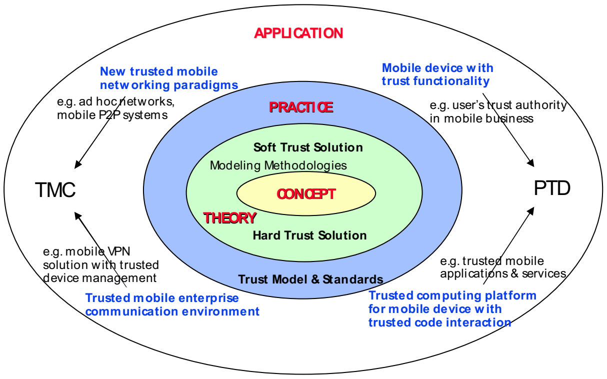
APPLICATION
New trusted mobile networking paradigms
Mobile device with trust functionality
e.g. ad hoc networks, mobile P2P systems
PRACTICE
e.g. user's trust authority in mobile business
Soft Trust Solution
Modeling Methodologies
CONCEPT
THEORY
Hard Trust Solution
TMC
PTD
e.g. mobile VPN solution with trusted device management
Trust Model & Standards
e.g. trusted mobile applications & services
Trusted mobile enterprise communication environment
Trusted computing platform for mobile device with trusted code interaction

Figure 1: A conceptual architecture of a trusted mobile environment

Trust is a very complicated phenomena attached to multiple disciplines and influenced by many subjective and objective factors. Therefore, it is essential to define a conceptual architecture to clarify target scenarios, thus narrow down our study and make it easy to focus on the concrete issues in different aspects of the trusted mobile environment.

We propose an onion structure, as shown in Figure 1. It is composed of four circles. A concept circle is at the core of the onion. This circle defines a series of concepts about trust, its derivatives and its related terms. Based on the working concepts, theories and modeling methodologies can be built upon, forming a theory circle. Outside the theory circle, there is a practice circle. The practice circle applies theories and methodologies into various trust models and standards for supporting the trust in real applications and systems that form its outer circle: an application circle.

2.1. Definitions – concept circle

Due to multiplicity of meanings associated with the word 'trust' and its derivatives, it is essential to establish a certain set of definitions that can be used throughout the work towards the trusted mobile environment. A series of working definitions build up the core part of the proposed architecture.

The first concept to clarify is the ‘trust’. Based on the literature study, we found that trust is defined in various ways for different purposes, even though in information technology area. Thereby it is difficult to have a common definition for this comprehensive concept. But the emphasized characteristics can be summarized. First of all, trust is subjective. That is the level of trust considered sufficient is different for each individual in a certain situation. Secondly, trust is dynamic as it is affected by many factors that are hard to monitor. It can be further developed due to positive experience. It is sensitive to be influenced due to negative experience. Finally, trust is trustor’s expectation or assessment on trustee regarding the properties of trust referent. It can be modeled, specified and verified in order to establish the trust [11].

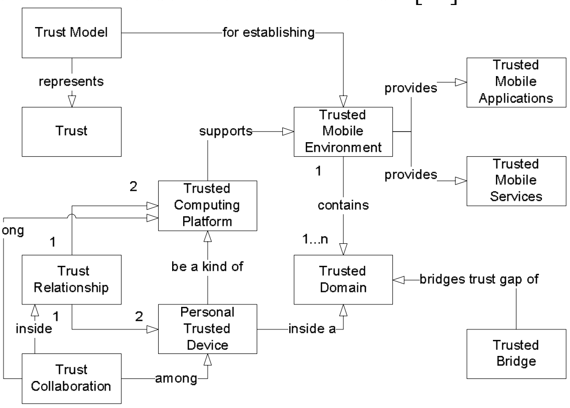

Figure 2: Relationships of concepts

Towards our purpose, we define a number of concepts. Their relationships are described in Figure 2. We define *trust* as the confidence of Entity A on another Entity B based on the expectation that Entity B will perform a particular action important to Entity A (trustor) [12]. The trustor could be a mobile device user, an enterprise company or a terminal node in an ad hoc network. The trustee could be a mobile device, a computing platform or a system providing various services. In order to evaluate trust in the mobile environment, we need to model trust, and thus to evaluate it and ensure it. *Trust modeling* is a technical approach to represent trust for digital processing. A *trust model* specifies, evaluates and sets up trust relationships among entities.

Regarding a *trusted mobile environment* for mobile services and applications, we refer to an infrastructure that can support trusted mobile applications and services, which make use of mobile devices as user agents, deploy various wireless networks as communication channels and apply mobile communication technologies as basic measures. The *mobile services* can be vaguely defined as services that are provided to mobile users via mobile devices [12], e.g. a mobile ticketing service. The *mobile applications* are the software applications installed and executed at the mobile devices, which may run independently or have communication capability to contact local or remote devices. A Java MIDlet is one type of a mobile application.

Generally, a mobile environment is composed of a number of trusted domains. 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 a specified purpose, and all domain components adhere to such trust definition and implement the statements. A defining statement identifies requirements of the domain entities to be trusted, and must be fulfilled by the domain components. The trusted mobile environment can be established when those trusted domains collaborate together through bridging trust gaps among them. 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 trust or bridge trust gaps among those domains.

Inside a trusted mobile environment, a mobile device with a computing platform plays a key role. Regarding a *trusted computing platform* (TCP), it must behave in a way as it is expected to behave for an intended purpose. A *Personal Trusted Device* (PTD) is a platform device that accepts multiple technologies with special focus on mobile communications and falls in its user's personal trusted domain [12].

Among mobile devices and fixed devices in a communication scenario, *trust collaboration* is also required to ensure that interaction and cooperation are conducted according to the expectations of involved entities. For example, the shared contents in peer-to-peer systems should be consumed and operated following the content originator's or right-holder's expectation without violating any copyrights. In the peer-to-peer systems, the trust collaboration requires autonomous control over resources initiated by any one peer at any remote peer.

Since trust is dynamic, the established trust relationship could be changed due to varied environment. A *trust relationship* should be established between the trustor A and the trustee B and sustained for the fulfillment of an intended purpose. A *dual trust relationship* refers to the trust relationships that are established from the trustor A to the trustee B and from the trustee B to the trustor A.

2.2. Theory and modeling methodology – theory circle

Theoretically, there are two basic approaches for building up a trust relationship. We name them as a 'soft trust' solution and a 'hard trust' solution, as shown in Figure 1. The 'soft trust' solution provides trust based on trust evaluation according to subjective trust policies, facts from previous experiences and history. The 'hard trust' solution builds up the trust through structural and objective regulations, standards, as well as widely accepted rules, mechanisms and sound technologies. Possibly, both approaches are applied in a real system.

There are various ways of trust modeling for different system scenarios. The trust modeling is crucial for applying trust-building approaches into mobile systems. Regarding the trust analysis and modeling, we need special methodologies, which we will further discuss in section 3.1. In order to apply the 'hard trust' solution, it is essential to analyze default trust relationships among system entities and study potential changes of the trust relationship after the system initiation. Thereby, trust solutions to overcome trust gaps in the underlying system could be designed based on the existing regulations, standards, and widely accepted rules and technologies. For the 'soft trust' approach, it is important to clarify the border of entities or domains among which the trust evaluation is needed. Based on timely trust evaluation, decision could be made to apply appropriate mechanisms to ensure the trust relationship.

2.3. Trust models and standards – practice circle

Based on the theory and methodology established, we can design the trust models for typical mobile applications and systems. Thus corresponding standards can be made in industry to support real applications.

For example, the trust model of existing TCP in [13] is that the basic trust of every entity is rooted from sound hardware security – a 'hard trust' solution. Based on this root trust, further trust can be built on local OS and application software through authenticated booting. Trust on remote platform can be built on attestation of expected platform configurations.

2.4. Mobile applications and systems – application circle

This circle considers mobile applications and systems. We divide the application circle into four directions, as shown in Figure 1. Each direction implies motivations for potential business.

- Trusted computing platform for mobile devices with trusted code interaction: This direction aims to provide a TCP for mobile devices in order to support mobile applications and services in a secure and trustworthy way. It also ensures trustworthy device internal operation in a dynamically changed context.
- Mobile device with trust functionalities: This direction tries to provide the trust functionalities into mobile devices. With the new trust features, the devices will become more intelligent to interact with the users and behave as their trust advisors to help them make trust related decisions in mobile communications and personal business. With the TCP

support and the embedded trust functionalities, the future mobile device could become a PTD that could be the user's trust authority for various usages.

- New trusted mobile networking paradigms: This direction aims to support new mobile networking paradigms, such as MANET and mobile P2P systems. This kind of new networking paradigms holds special characteristics that introduce new challenges to security and trust.
- Trusted mobile enterprise communication environment: This direction is towards building up a trusted environment for mobile working and enterprise management, e.g. a mobile virtual private networking (VPN) solution with trusted device management. With the trusted mobile networking in both public domain and enterprise domain, a trusted mobile communication (TMC) environment could be supported.

3. Key Motivations

By further developing the presented architecture, we can identify the motivations of our main efforts. In this section, we further discuss a number of key motivations for the trusted mobile environment.

3.1. Modeling methodologies and toolkit

First of all, we need methodologies to model trust for an intended purpose, and thus to build up a trusted system by applying the model. There are various methodologies can be applied for solving different issues. Some trust models are based on sound technologies, e.g. PKI [3]. A big number of trust models are built up targeting at some trust properties, such as reputations, recommendations and risk [14, 15]. Many trust models have been constructed for various computing paradigms such as GRID computing, ad hoc networks, peer-to-peer networks, and multi-agent systems, etc [16-18]. In those models, some are computational, others are linguistic or graphic. For example, in [19], subjective logic is used to assess trust values based on the triplet representation of trust. In [20], linguistic trust metrics are used for reasoning trust with provided rules. In the context of the "Web of Trust," many trust models are built upon a graph where the resources/entities are nodes and trust relationships are edges, such as in [21].

Although a variety of trust models are available, it is still not well understood what fundamental criteria the trust models must follow. Without a good answer to this question, the design of trust models is still at the empirical stage [22]. Current work focuses on concrete solutions in special systems. Particularly, there is no feasible trust modeling methodologies available that can be applied into mobile domains in a common way. Thus it lacks general instructions when we are designing, analyzing and developing a trusted mobile system.

Taking a mobile communication system as an example, we can find many cases in which a system is actually formed by a number of trusted domains. The communications are actually conducted among and across those domains. Inside each trusted domains, the trust relationships exist among the domain entities. But among the domains, a significant problem may arises from the fact that the different domains deficient of trust must cooperate in order to provide a complete service even though they may not share the same concept of trust. Specifically, frequent security problems among those domains may be caused by the deficiency of trust among domains. This deficiency is probably one of the major barriers that prevents for the proliferation of the mobile communications and services.

Based on the above analysis, a mobile communication system can be modeled into a number of trusted domains. Inside a trusted domain, the trust relationship exists. While among the domains, trust is lacking, and needs special technologies to build up. One of the solutions is presented in our previous work [12]. Specifically, the modeling methodology falls into the theory circle. It is also related to the practice circle because a new trust model for a mobile communication system is generated based on the methodology.

From system design point of view, the industry lacks a toolkit that could help on designing a trusted mobile system. The toolkit provides methods to analyse target system and find the potential trust deficiency. In addition, it provides a number of technologies to make up the trust deficiency. More importantly, the toolkit offers a mechanism to evaluate multiple solutions, thus helping the designer to select an optimised one as the final solution. Regarding the system software implementation, the toolkit further helps on designing trusted system software by modeling, specifying and verifying trust in software architecture and software programming.

3.2. Personal trusted device

The second issue is how to provide a personal trusted device for the mobile users. It is the key element for building up a trusted mobile environment. This is because trust establishment in mobile domain greatly relies on the mobile devices.

There are three issues needed to solve herein. Firstly, we need a trusted computing platform with trust code interaction for the mobile device in an efficient way. The mobile device platform layer should provide essential security services, such as authenticated booting, encryption service, secure storage, privacy support and digital rights management. Trusted Computing Group (TCG) set its goal towards maintaining the privacy of the platform owner while providing a ubiquitous interoperable mechanism to validate the identity and integrity of a computing platform [13]. However, due to the small size of mobile devices, this technology needs to be adapted for hand-held products. This work is still on going at TCG.

In addition, the platform runtime layer should provide a mechanism to support trustworthy cooperation of multiple software components, thus ensure device applications can be executed as required and expected regarding system dependability, security and adaptability. The device platform is capable to monitor system performance and adaptively arrange limited device resources (such as power, memory, network capability and CPU) in order to fulfill trust requirements of different applications and services even though in a dynamically changed environment. The platform could further overcome system threats in a prevented and tolerant measure. It should be adaptive to the changes of software running environment due to new components execution and old one's deletion, as well as the changes raised outside the device. Based on our literature study, little work is done in this area, especially for the mobile devices [23].

Secondly, the device should be intelligent as a personal trust advisor for its user's personal business. It contains the user's criteria of the trust in different circumstances. It has capability to collect, codify, analyze, and present evidence relating to competence, adaptability, security or dependability with the purpose of making evaluation and decisions regarding trust relationships for mobile applications and services, as well as mobile networking. Regarding this requirement, initial work is presented in [24], however no further concrete solution follows. A big number of trust management solutions are presented for trusted communications in MANET and mobile P2P systems based on distributed trust models [25, 14, 17, 18]. However, very little research is conducted about how mobile device users should manage and use these kinds of systems or how well they really work in practice.

Thirdly, we need the PTD to ensure the trust relationship to be established for the intended purpose and sustained until the purpose is fulfilled. This is crucial for trusted mobile commerce and services. In one word, the PTD will become the mobile user's trust authority in mobile commerce and communications. The TCP was proposed to improve the trust between users and their devices. The TCG's TCP technology ensures this through a set of hardware and software mechanisms. However, current work on TCP lacks solutions for trust sustaining among TCPs, so that trust loyalty might be broken after a period of time. In order to solve this problem, we presented a mechanism for sustaining trust among TCPs in [26].

3.3. Trusted mobile communications

The third issue is how to provide the trusted mobile communications in both a dynamically changed public domain and an organization's enterprise domain.

In the public domain, future mobile networking is most possibly in an ad hoc style organized by mobile devices randomly. Operation in an ad hoc network introduces new security problems. The ad hoc networks are generally more prone to physical security threats. The possibility of eavesdropping, spoofing, denial-of-service, and impersonation attacks increases. But security approaches used for the fixed networks are not feasible due to the salient characteristics of the ad hoc networks. New threats, such as attacks raised from internal malicious nodes, are hard to defend against. New security mechanisms are needed to adapt to the special characteristics of the ad hoc networks. A trust evaluation based security solution (a 'soft trust' solution) could be an effective approach for data protection, secure routing and other network activities [25]. It can also cooperate with a TCP based 'hard trust' solution to provide improved trust in the MANET. Combined solution is seldom studied in the literature and practiced in industry.

In the enterprise domain, trust plays a key role in the context of VPN. However, providing advanced trust into mobile VPN networks has proven to be problematic. Generally, a mobile enterprise networking is composed of various devices provided by different vendors with different security support. Trust management on confidential digital contents at different enterprise devices in different domains (e.g. a public networking domain and a virtual private network domain that are either trusted or distrusted) is a new challenge worth special efforts.

4. An Example

In this section, we evaluate the architecture's expressiveness and advantages by applying it into a mobile peer-to-peer system.

Mobile peer-to-peer computing has emerged as a significant paradigm for providing distributed services, in particular collaboration for content sharing and distributed computing. Generally, a mobile P2P system consists of a decentralized and self-organizing network of autonomous devices that interact as peers. Each peer acts as both client and server to share its resources with other peers. However, this computing paradigm suffers from several drawbacks that obstruct its wide adoption.

Lack of trust between peers is one of the most serious issues, which causes security challenges in the P2P systems. Building up trust collaboration among the system peers is a key issue to overcome.

Based on the proposed architecture, we presented a trusted collaboration infrastructure for a mobile P2P system in [27]. This infrastructure combines both the 'soft trust' solution and the 'hard trust' solution in order to support the trust collaboration among the mobile peers. We applied the same concepts defined in the concept circle. By using the modeling methodology introduced in 3.1, the system can be modeled as a number of trusted domains – trust bubbles. As shown in Figure 3, each peer device is independently located inside a personal trusted bubble: the basic unit that represents a peer. Inside the bubble, the owner of the peer device trusts the device based on the PTD technology. The device is responsible for the communication with other peers. Among bubbles, logical and rational trust relationships should be attested. In order to build up the trust collaboration among the bubbles, we applied both the 'hard trust' solution and the 'soft trust' solution.

The 'hard trust' solution is an improved TCP technology that can ensure the trust sustainability. The trust relationship can be established between a trustor device and a trustee device based on the device platform attestation and the registration of trust conditions at the trustee device's TCP components. With the TCP components inside the peer device, a trustee device can ensure the trust sustainability according to pre-defined conditions. The conditions are approved by both the trustor device and the trustee device at the time of trust establishment. They can be further enforced through the use of the pre-attested TCP components at the trustee device until the intended collaboration is fulfilled. The TCP components are built in the secure hardware chip, which is very hard to be broken, even by the trustee itself.

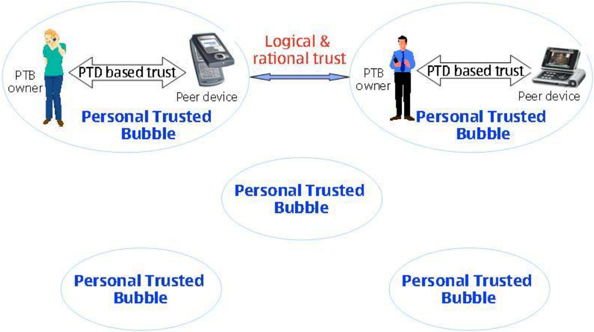

Figure 3: Trust model of a mobile peer-to-peer system

Regarding the 'soft trust' solution, the trust evaluation mechanisms embedded in each peer device can anticipate potential risks and make the best decision on any security related issues in the P2P communications and collaborations. The trust evaluation results can help generating feasible conditions for sustaining the trust relationship. This mechanism is very helpful in fighting against attacks raised by internal malicious peers that hold a correct platform certificate and valid data for trusted platform attestation.

Through defining the basic concepts and using the modeling methodology, we model the system trust and clarify where problems exist and solutions should be applied. By making use of the technologies specified in the theory circle, we can establish the trusted mobile communications in a mobile P2P system. The presented architecture facilitates our work in understanding, analyzing and solving the trust issues.

5. Conclusions

Trust is playing and will continuously play an important role in digital services and applications. This crucial influence has been extended into the mobile domain. In order to support further success of mobile communications, applications and services, it is significant to study trust issues for providing a trusted mobile environment. This environment aims to offer trusted interaction among the mobile devices and their internal components, trust collaboration among mobile communication peers, and trust-intelligence support for the users at the mobile devices.

The paper presented a conceptual architecture for establishing the trusted mobile environment. This architecture clarified the structure of trust issues in different aspects of the mobile environment. Based on the architecture, we specified the key motivations. Firstly, we need the trust modeling methodologies for analyzing trust issues. Secondly, we depend on the PTD with trusted computing platform and trust functionalities to behave as the user's trust authority in the mobile networking and services. Finally, the trust management plays an important role in the mobile communications in order to overcome new challenges. In order to evaluate the architecture, we further apply it into a mobile P2P system to demonstrate its expressiveness and advantages.

References

[1] L. Zhou, Z.J. Haas, "Securing Ad Hoc Networks", *IEEE Network*, 13(6): 24-30, Nov/Dec 1999.

[2] D.H. McKnight, N.L Chervany, "What is Trust? A Conceptual Analysis and An Interdisciplinary Model", *Proceedings of the 2000 Americas Conference on Information Systems* (AMCIS2000), Long Beach, California, August 2000.

[3] R. Perlman, “An Overview of PKI Trust Models”, *IEEE Network*, vol.13, no.6, Nov.-Dec. 1999, pp. 38-43.

[4] T. Grandison, M. Sloman, “A Survey of Trust in Internet Applications”, IEEE Communications and Survey, Forth Quarter, 3(4), 2000, pp. 2–16.

[5] Y. Tan, W. Thoen, “Toward a Generic Model of Trust for Electronic Commerce, *International Journal of Electronic Commerce* vol.5, no.2, 1998, pp. 61-74.

[6] A. Alfarez, H. Stephen, “A Distributed Trust Model”, *Proc. of New Security Paradigms Workshop*, ACM, New York, NY, USA, 1998.

[7] S.J. Vaughan-Nichols, “How trustworthy is trusted computing?” *Computer*, Volume 36, Issue 3, March 2003.

[8] P. England, B. Lampson, J. Manferdelli, M. Peinado, B. Willman, “A Trusted Open Platform”, *IEEE Computer Scciety*, July 2003, pp. 55-62.

[9] D.W. Manchala, “E-Commerce Trust Metrics and Models”, *IEEE Internet Computing*, vol.4, no.2, 2000, pp. 36-44.

[10] M. Lik, M. Mojdeh, H. Ari, “A Computational Model of Trust and Reputation”, *Proc. Of the 35th Annual Hawaii International Conference on System sciences*, Big Island, HI, USA, January 2002.

[11] DE Denning, “A new paradigm for trusted systems”, *Proceedings of the IEEE New Paradigms Workshop*, 1993 - portal.acm.org.

[12] Z. Yan, P. Cofta, “Methodology to Bridge Different Domains of Trust in Mobile Communications”, *The First International Conference on Trust Management*, Crete, Greece, May 2003.

[13] TCG TPM Specification v1.2, 2003. https://www.trustedcomputinggroup.org/specs/TPM/

[14] L. Xiong, L. Liu, “A Reputation-based Trust Model for Peer-to-Peer E-commerce Communities”, *IEEE International Conference on E-Commerce*, CEC 2003, pp. 275 – 284.

[15] Z. Liang, W. Shi, “PET: A PErsonalized Trust Model with Reputation and Risk Evaluation for P2P Resource Sharing”, *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, Jan. 2005, pp. 201b - 201b.

[16] Z. Zhang, X. Wang, Y. Wang, “A P2P Global Trust Model Based on Recommendation”, *Proceedings of 2005 International Conference on Machine Learning and Cybernetics*, Vol. 7, Aug. 2005, pp.3975 – 3980.

[17] G. Theodorakopoulos, J.S. Baras, “On Trust Models and Trust Evaluation Metrics for Ad HocNnetworks, *IEEE Journal on Selected Areas in Communications*, Vol. 24, Issue 2, Feb. 2006, pp. 318 – 328.

[18] C. Lin, V. Varadharajan, Y. Wang, V. Pruthi, “Enhancing Grid Security with Trust Management”, *Proceedings of IEEE International Conference on Services Computing* (SCC 2004), Sept. 2004, pp. 303 – 310.

[19] A. Jøsang, “An Algebra for Assessing Trust in Certification Chains,” *Proc. Netw. Distrib. Syst. Security Symp.*, 1999.

[20] D. W. Manchala, “Trust Metrics, Models and Protocols for Electronic Commerce Transactions,” *Proc. 18th IEEE Int. Conf. Distrib. Comput. Syst.*, May 1998, pp. 312–321.

[21] M. K. Reiter, S. G. Stubblebine, “Resilient Authentication Using Path Independence,” *IEEE Trans. Comput.*, vol. 47, no. 12, Dec. 1998, pp. 1351–1362.

[22] Y. Sun, W. Yu, Z. Han, K.J.R. Liu, “Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks”, *IEEE Journal on Selected Area in Communications*, Vol. 24, Issue 2, Feb. 2006, pp. 305 – 317.

[23] M. Zhou, H. Mei, L. Zhang, “A Multi-Property Trust Model for Reconfiguring Component Software”, *Fifth International Conference on Quality Software QAIC2005*, Sept. 2005, pp. 142 – 149.

[24] P. Cofta, S. Crane, “Towards the Intimate Trust Advisor”, *The First International Conference on Trust Management*, Crete, Greece, May 2003.

[25] Z. Yan, P. Zhang, T. Virtanen, “Trust Evaluation Based Security Solution in Ad Hoc Networks”, *The Seventh Nordic Workshop on Secure IT Systems* (NordSec03), Gjövik, Norway, October 2003.

[26] Z. Yan, P. Cofta, “A Mechanism for Trust Sustainment among Trusted Computing Platforms”, *The First International Conference on Trust and Privacy in Digital Business* (TrustBus’04), Spain, September 2004.

[27] Z. Yan, P. Zhang, “Trust Collaboration in Peer-to-Peer Systems Based on Trusted Computing Platform2, *WSEAS Transactions on Information Science and Applications*, Issue 2, Vol. 3, February 2006, pp. 275-282.