Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers, Tenerife, Spain, December 16-18, 2005 (pp190-196)

Building up Trust Collaboration in P2P Systems Based on Trusted Computing Platform

ZHENG YAN, PENG ZHANG
Nokia Research Center, Nokia Enterprise Solution
Itämerenkatu 11-13, Helsinki, FINLAND

Abstract: - Peer-to-peer computing has emerged as a significant paradigm for providing distributed services, in particular collaboration for content sharing and distributed computing. 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. This paper studies the feasibility to build up trust collaboration based on Trusted Computing Platform (TCP) in peer-to-peer systems. Based on analysis, the authors conclude that the TCP technology is a promising solution that can overcome many P2P security challenges, thus realize trust collaboration among P2P peers.

Key-Words: - Trust collaboration, Peer-to-peer, Trusted computing platform

1 Introduction

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 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.

Peer-to-peer computing has significant benefits including scalability, low cost, robustness and ability to provide site autonomy. However, this approach suffers from several drawbacks that influence its wide adoption. Security is one of main challenges that retard its wide usage [1, 2].

There are a number of reasons why security is crucial in the P2P systems. Firstly, downloading files from other machines makes the systems vulnerable to viruses. Secondly, it is important that communicating computers or devices have the ability of authenticating the identity of each other when they engage in collaboration. Thirdly, the availability of resources is seriously threatened by DoS attacks through overloading some nodes. Generally, it is difficult to fight attacks raised from internal malicious peers. Fourthly, when online users become more concerned about privacy, some of them may hesitate to use the P2P services. They will not accept a technology if personal information will be exposed without any control. A more secure P2P infrastructure is expected. Finally, intellectual property management and digital rights management (DRM) are highly required in P2P systems. We have to restrict access to shared contents according to copyrights and legal usage rights. Flexible DRM control is a necessity in the P2P systems.

The whole P2P network environment is made up of heterogeneous hardware and software components with dynamic capability. The peers holding different local policies could come and leave the network randomly. Such system lacks trust among peers since access resources must be granted to unknown peers. Fundamentally, sharing and making use of resources requires collaboration among peers in the P2P systems. The key to solve above security problems is to build up trust collaboration in the P2P systems.

This paper presents applying trusted computing platform technology into the P2P systems in order to support trust collaboration among peers towards autonomous resource management. The paper is organized as follows. Based on the introduction of trust computing technology in section 2, we propose a trusted collaboration infrastructure (TCI) based on TCP in Section 3. The architecture is analyzed in section 4. Section 5 discusses some related work, followed by conclusions provided in the last section.

2 Trusted Computing Platform

The current technologies for trusted computing platform are quite similar [3, 4]. The typical TCP technologies are specified in the specifications of TCG (Trusted Computing Group) [5]. TCG aims to enhance the overall security, privacy and trustworthiness of a variety of computing devices.

TCG's Trusted Computing Platform (TCP) builds its promise of a trusted platform on the basis

of some hardware – the Trusted Platform Module (TPM). In short, TPM is the hardware that controls the boot-up process. Every time the computer is reset, the TPM steps in, checks itself and then verifies the OS loader before letting boot-up continue. The OS loader is assumed to verify the operating system (OS), the operating system is assumed to verify every bit of software that it can find in the computer, and so on.

The TPM chip and other TCP modules simply allow all hardware and software components to check whether they have woken up in trusted states. If not, they should refuse to work. It also provides secure storage for confidential information. Simply speaking, there are four basic functions provided by TCP.

2.1 Authenticated booting

An authenticated boot service monitors what operating system software is booted and gives applications a sure way to identify which OS is running. Figure 1 illustrates the process of authenticated booting and trust challenge on remote platform or data.

A TPM chip takes charge when booting up. Its booting block checks the hardware specification against a known safe integrity metric; and should that match, it then checks the OS loader. The OS loader, once proven safe, checks the OS kernel. The kernel knows how to check the list of legitimate software, which in turn can use OS resources to authenticate local and remote data [5].

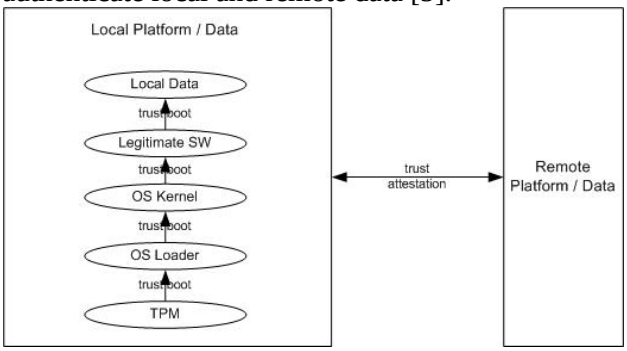

Fig. 1: Authenticated booting and remote platform trust attestation

What is more, the TCP hardware can make the configuration known to others, thus realize the trust attestation on remote platform/data. This is done through digitally certificating the configuration. Two levels of certifying are provided. The TPM certifies that a known OS version is running and then the OS can certify the application's precise configuration.

2.2 Encryption service

Encryption service is the second major offer of TCP. It allows data to be encrypted in such a secure way that it can be decrypted only by a certain machine, and only if that machine is in a certain configuration.

This service is implemented by a combination of hardware and software facilities. The TPM hardware maintains a 'master secret key' for each machine, and it uses the master secret to generate a unique secret encryption key for every possible configuration of that machine. Thus, data encrypted for a particular configuration cannot be decrypted when the machine is in a different configuration.

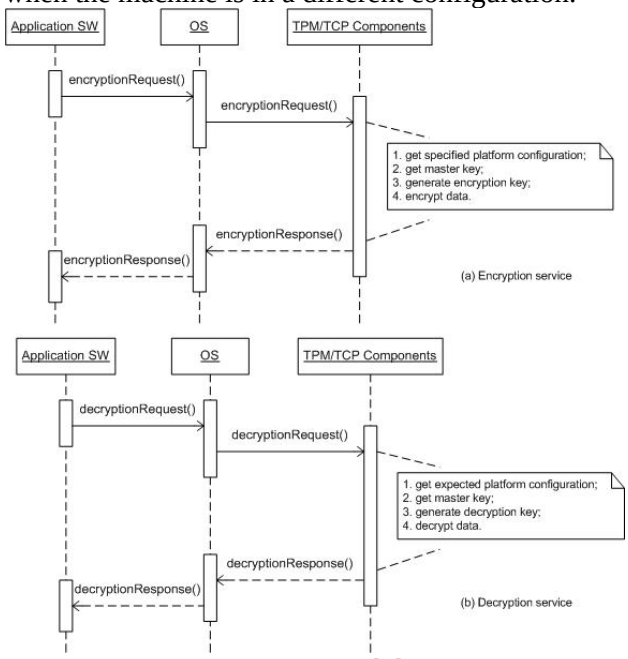

Fig. 2: Encryption service and decryption service offered by TCP components

This service can be extended from OS level to applications. This ensures that encrypted data can only be decrypted by desired version of desired applications when running on top of desired OS and on desired machine. So, we can transmit data to a remote machine in such a way that the data can be decrypted only if the remote machine is in a certain configuration. Figure 2 briefly show the encryption service and corresponding decryption service provided by the TCP components. The encryption service provides a special control on digital data to make it accessible only when an expected platform environment is present.

2.3 Privacy support

The TCG specification provides a method described below for obtaining an anonymous user identity certificate from a Certificate Authority (CA) over a secure channel.

The TPM sends the public key (of the user that desires a certificate) and three credentials to the CA. The three credentials include:

- *A public key certificate*: the endorsement certificate issued by the entity that endorses or certifies the TPM. It contains a null subject and the TPM endorsement identity's public key, among other things.
- *The first attribute certificate*: the platform credential containing a pointer to the endorsement certificate that uniquely identifies the platform's endorser and the model – hardware and software versions, TPM details, platform compliance with the TCG specifications, etc.
- *The second attribute certificate*: the conformance credential, that asserts that the named TPM complies with the TCG specification.

The CA receives these three certificates, and verifies the information. Then the CA creates a TPM identity credential and sends it to its client via the secure channel. The TPM identity credential contains a null subject and the public key sent by the user in the certificate request. This procedure ensures that anonymous certificates are only issued to compliant devices.

2.4 DRM support

The TCG specifications present several problems regarding to DRM. A TCG-enabled OS could prevent the user from running "unapproved" applications. Thus the applications with capability for copying, printing, and super-distributing digital contents are not allowed to play DRM-sensitive contents. Through extending the encryption service offered by the TCP, the TCG-enabled computing platform could control digital contents access and execution; master the usage of software programs as well as the operation of the system according to the specified rules.

3 Building up Trust Collaboration on TCP

With TCP compatible devices in the P2P system, it will be easy to build up trust collaboration to support secure P2P applications. In what follows, we propose a P2P infrastructure based on TCP and analyse how this infrastructure can solve the security problems listed in section 1, therefore support trust collaboration in the P2P systems.

3.1 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.

Trust is the confidence of an entity (trustor) on another entity (trustee) based on the expectation that the trustee will perform a particular action important to the trustor, irrespective of the ability to monitor or control the trustee [19].

Trust modeling is a technical approach to represent trust for digital processing. A trust model specifies, evaluates and sets up trust relationships among entities [19].

Trusted computing platform is a computing system behaving in a way as it is expected to behave for a intended purpose [5]. The TCG's TCP technology ensures this through a set of hardware and software mechanisms for authenticated booting, platform integrity attestation and access/operation control attached to platform specific configurations.

Trust collaboration is defined as interaction, communication and cooperation are conducted according to the expectation of involved entities. For example, the shared contents in the P2P systems should be consumed and used following the content originator's or right-holder's expectation without violating any copyrights. In peer-to-peer systems, the trust collaboration requires autonomous control on resources at any peer.

3.2 Trust modeling

We model the trust of the P2P system according to its specific characteristics described in the introduction. 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 illogically trusts the device, which is responsible for the communication with other peers. Among bubbles, logical and rational trust relationships should be attested.

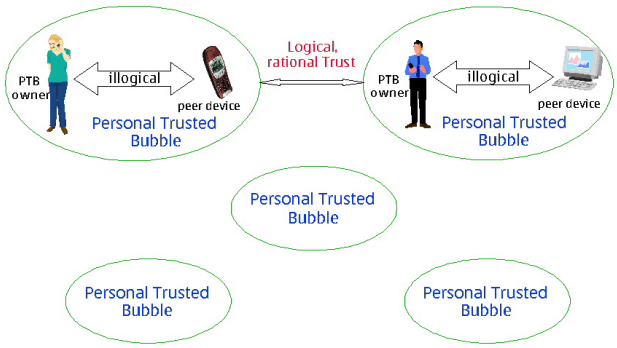

Fig. 3: Trust model of peer-to-peer system

3.3 Trusted collaboration infrastructure (TCI) for P2P

Based on the trust model, we further propose a trusted collaboration infrastructure (TCI) for the P2P system. In this infrastructure, each peer device is

TCP compatible and has an internal architecture as shown in Figure 4.

There are three layers in this architecture. Platform layer contains TCP components specified in [5] (e.g. TPM) and operating system that is booted and executed in a trusted status, which is attested and ensured by the TCP components.

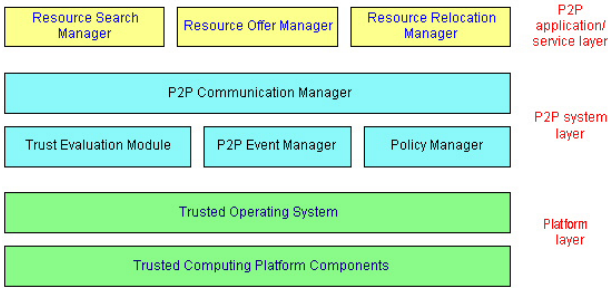

Fig. 4: Architecture of P2P peer device in TCI

P2P system layer contains common components required for trusted P2P communications. Those components are installed over the platform layer and ensured running in a trusted status. This is realized through trusted component installation and change-detection mechanism supported by the platform layer. Communication manager is responsible for various P2P communications (e.g., P2P system joining and leaving). Trust evaluation module is applied to evaluate trust relationship with any other peer before any security related decision is made. The trust evaluation module cooperates with policy manager and event manager in order to work out a proper trust evaluation result. The policy manager registers various local device policies regarding P2P applications and services. It also maintains subjective policies for trust evaluation. The event manager handles different P2P events and cooperates with the trust evaluation module in order to conduct proper processing.

P2P application/service layer contains components for P2P services. Taking resource sharing as an example, this layer should contain components like resource-search manager, resource-offer manager and resource-relocation manager. The resource-search manager is responsible for searching demanded resources in the P2P system. The resource-offer manager provides shared resources according to their copyright and usage rights. The offered resources could be encapsulated through the encryption service of TCP. The encryption is attached to some special configurations as mandatory requirements for decryption. The resource-relocation manager handles remote resource accessing and downloading. The downloaded resources are firstly checked with no potential risk, and then stored at the local device.

Like the system layer, all the components in this layer are attested by the platform layer (e.g. trusted OS) as trusted for execution. Any malicious change could be detected and rejected by the platform layer.

3.4 Trust collaboration

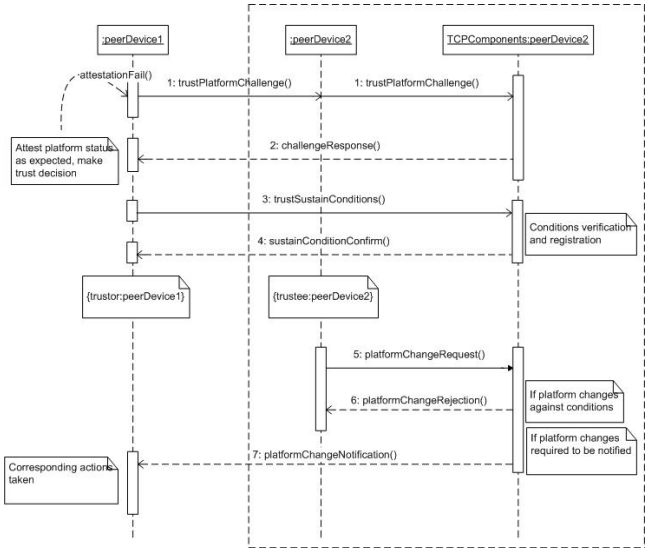

Fig. 5: Trust collaboration in P2P system

The trust collaboration in the proposed P2P system infrastructure is supported as follows:

- *Each peer device can verify that another peer device is working in its expected status.*

Building up on the TCP technology, each peer device with the underlying architecture can ensure every component on the device is working in a trusted status. It can also challenge any other device and attest that it is working in its expected status, as shown in Figure 5 (step 1 and 2).

- *Trust relationship established at the beginning of the collaboration between peers can be sustained until the collaboration is fulfilled for some intended purpose based on trust conditions.*

As shown in Figure 5, the trust relationship can be established between a trustor device and a trustee device based on the trust evaluation and platform attestation (step 1-4). With the TCP components inside the peer device, a trustee device can ensure the trust sustainment according to pre-defined conditions (step 5-6). The conditions are approved by both the trustor device and the trustee device at the time of trust establishment and enforced through the use of the pre-attested TCP components at the trustee 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. Through this mechanism, there are ways to automatically control the remote environment as trusted. It is also possible to inform the trustor peer about any distrust behavior of the trustee according to pre-defined conditions (step 7). Therefore, it is feasible for the trustor peer to take

corresponding measures to confront any changes that may affect the continuation of trust for the purpose of a successful P2P service.

- *Each peer can manage the trust relationship with other peers and therefore it can make the best decision on security issues in order to reduce the potential risks.*

Based on the trust evaluation mechanisms [6-8] embedded in the trust evaluation module, each peer can anticipate potential risks and make the best decision on any security related issues in the P2P communications and collaborations. It can help on making feasible conditions for sustaining the trust relationship based on the evaluation results. In addition, the trust evaluation is conducted in the expected trust environment, thus the evaluation results could be trusted. 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.

- *Resources are offered under expected policies.*

This includes two aspects. One is that the resources are provided based on copyright restrictions. Those contents that cannot be shared should not be disclosed to other peers. The other is that the resources are provided with some limitations defined by the provider. The encryption services offered by the TCP can cooperate with the resource-offer manager to provide protected resources and ensure copyrights and usage rights.

- *Resources are relocated safely and consumed as the provider expects.*

The trust attestation mechanism offered by the TCP can support the resource-relocation manager to attest that the downloaded contents are not malicious code. In addition, the resources are used in an expected way, which is specified according to either copyrights or pre-defined usage restrictions. This can be ensured ahead of consuming by the TCP encryption mechanism.

- *Personal information of each peer is accessed under expected control.*

The resource-offer manager in the proposed architecture can cooperate with the TCP components to encapsulate the personal information based on the policies managed by the policy manager. Only trusted resource-search manager can access it. The trusted resource-search manager is an expected P2P application component that can process the encapsulated personal information according to the pre-defined requirements specified by the personal information owner.

With the TCP components in the TCI, any P2P device component can and only can execute as expected and process resources in the expected way. Furthermore, with the support on the trust evaluation and trust sustainment, the peers could collaborate in the most trusted way.

4 Further Discussion on Security Challenges

In this section, we further discuss how the TCI based P2P systems could overcome security challenges presented in the introduction.

- Virus vulnerability

In the TCI, platform authenticated booting and remote platform attestation could ensure that any virus does not affect the underlying communicating platform. In addition, any downloaded file by the resource-relocation manager should be further attested by the TCP components to ensure that the code is safe. The hash code of expected data is used to conduct the verification. It is also possible for the TCI to ensure that the virus or malicious code does not infect the remote peer device through the trust sustaining mechanism during the peer collaboration.

- Identity authentication

TCP components provide secure storage to save a unique platform ID and also offer support to assign various aliases on this ID for privacy purposes. If every peer device is TCP compatible, they can authenticate with each other based on the platform ID and its alias.

- The risk raised by malicious peers could be greatly reduced based on the trust evaluation mechanism. The trust evaluation module requires sound protection to ensure its correct process. The TCP components in the proposed architecture provide a secure running environment and further ensure the integrity of this environment for the trust evaluation.

- One important mechanism that can be supported by the TCI is privacy. A different alias of the platform ID can be used for different purposes. The alias could be also attached to some specified platform configurations or application configurations to support restricted P2P services. In addition, the encryption service can also be applied into personal profile (that stores the user information) in order to control in which kind of situation, the information inside the profile can be accessed.

- DRM is strongly supported in the TCI based P2P systems through encryption service mechanism. Most importantly, this mechanism can be further extended to attach encryption to specified usage rights and specified content consuming software to

ensure the expected consuming environment of the shared contents.

5 Related Work

There is some related work conducted in the literature.

In [9], an open-source framework JXTA was proposed to support programming secure peer-to-peer applications. It contains a set of protocols to realize secure peer-to-peer connection. It also supports certificates provided by peers, which behave as the internal CA. This programming platform is based on the Java technology, which is a pure software solution on P2P security. However, it lacks support on DRM, virus control and private data Spam, but the TCI solves.

In [7], the MOTION architecture was proposed to realize access control over mobile P2P environment. But it has no support on autonomous access control over already shared resources.

In [10], collaboration is thought as humans involved in the P2P systems interacting with each other in a near real-time manner. The concept of collaboration is different from what we defined in Section 3. In this paper, we pay more attention to the collaboration that can be conducted automatically among P2P devices. Two collaboration frameworks were introduced in [10]: Endeavors and Avaki. Both frameworks and the Proem architecture introduced in [8] build upon a software platform and use a software solution to control access. But they cannot automatically support access control on remote resources that have been shared during network collaboration.

In [11], a hybrid architecture mixing a trusted centralized control with distrusted peer-to-peer components was proposed for an enterprise P2P scenario. In this architecture, distributed resource usage is adaptive to the trustworthiness of the distributed components. The central control component is in charge of coordinating the interaction with the external services and the distrusted peer-to-peer components. In this model, the overall architecture is adaptive to trust and reliability assessment. Trust of a distrusted component is assessed through evidence collection. However, this paper did not discuss how to protect trust assessment and how to sustain trust if the peer components disconnected from the central-control component, both of which are considered in the TCI.

There is some work on building up a new trust model for the P2P systems. In [12], a trust model based on trust-based group (*troups*) is suggested. This model supports transitive trust. But this model needs special protocol to support dynamic membership inside the *troups*. Compared to our trust model, this model is more complicated to manage. According to [13], trust is not always transitive. Therefore this model needs further study in order to prove the transitivity property.

A line of trust modeling work for P2P systems is based on reputation [14-16], in which reputation is the main factor that is deployed for trust evaluation among peers or domains. Its trust modeling is similar to ours. But the trust building in this kind of P2P systems depends on reputation based trust management, not on a trusted computing platform. In our design, we make use of trust evaluation among peers to reduce risks raised by malicious peers, while build up trust collaboration based on a uniform TCI support. This is more feasible in practice, especially in mobile domains because collecting valuable information for trust evaluation is a challenge in the mobile P2P scenarios.

In [17], a protocol for anonymous trust management was proposed. It provides mutual anonymity for both trust host (that manages the trust ratings of the P2P peers) and trust querying peer in order to secure trust management in P2P distributed systems. Our proposal is different from this solution in that each peer is supposed to run independently and anonymously if needed. In addition, our proposal is supported by uniform platform architecture, not a protocol.

In summary, existing work has not studied how to effectively support trust collaboration among the peers in a P2P system. Especially, the automatic resource management across peers is lacked in consideration.

6 Conclusions

TCP technologies are under-development in industry and academy in order to provide more secure and better trust support for future digital devices. TCP tries to solve existing security problems by hardware trust. Although it is still in its infancy and may be vulnerable to some hardware attacks [18], it has advantages over many software-based solutions. One important work at present is the study on how to enforce the trust relationship between device OS and applications and among different application layers with sound performance, especially when the device is a small mobile terminal with some limitations.

In this paper, we introduced a perspective of building up trust collaboration in a P2P system

based on the trusted computing platform. Through a uniform TCP compatible P2P device architecture, many security challenges presented in the introduction can be overcome. In addition, the proposed TCI based P2P system can also support automatic network resource management as well as privacy. It provides a series of platform mechanisms for people to select in order to realize personal protection purpose. Therefore, it greatly supports the trust collaboration in the P2P networks lacking trust. It has potential advantages over other solutions; especially when the TCG standard is deployed and many industry digital device vendors (e.g. Microsoft, IBM, HP, Intel, etc.) offer TCP-compatible hardware and software in the future.

Acknowledgments

The authors would like to thank Olli Immonen and Silke Holtmanns for their valuable comments.

References:

[1] D. Clark, Face-to-Face with Peer-to-Peer Networking, *Computer*, Vol. 34, No.1, Jan. 2001, pp.18-21.

[2] Daswani Neil, Garcia-Molina Hector and Yang Beverly, Open Problems in Data-Sharing in Peer-to-Peer Systems, In *ICDT*, 2003.

[3] Edward W. Felten, Understanding Trusted Computing – Will it Benefits Outweigh Its Drawbacks, *IEEE Security & Privacy*, May/June 2003.

[4] England Paul, Lampson Butler, Manferdelli John, Peinado Marcus, Willman Bryan, A Trusted Open Platform, *IEEE Computer Society*, July 2003, pp. 55-62.

[5] Trusted Computing Group (TCG), TPM Specification, version 1.2, 2003.
https://www.trustedcomputinggroup.org/specs/TPM/

[6] Yan Z., Zhang P., and Virtanen T., Trust Evaluation Based Security Solution in Ad Hoc Networks, *The Seventh Nordic Workshop on Secure IT Systems*, NordSec 2003, Oct. 2003.

[7] Fenkam, P., Dustdar, S., Kirda, E., Reif, G., Gall, H., Towards an access control system for mobile peer-to-peer collaborative environments, *Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, June 2002, pp. 95 –100.

[8] Gerd Kortuem, Jay Schneider, Dustin Preuitt, Thaddeus G. C. Thompson, Stephen Fickas, Zary Segall, When Peer-to-Peer comes Face-to-Face: Collaborative Peer-to-Peer Computing in Mobile Ad hoc Networks, *The First International Conference on Peer-to-Peer Computing* (P2P01), Aug. 2001.

[9] Yeager, W., Williams, J., Secure peer-to-peer networking: the JXTA example, *IT Professional*, Vol. 4 Issue 2, March-April 2002, pp. 53 –57.

[10] Barkai, D., Technologies for sharing and collaborating on the Net**,** *Proceedings of First International Conference on Peer-to-Peer Computing*, Aug. 2001, pp. 13 –28.

[11] Mont, M.C., Tomasi, L., A distributed service, adaptive to trust assessment, based on peer-to-peer e-records replication and storage**,** *Proceedings of The Eighth IEEE Workshop on Future Trends of Distributed Computing Systems*, 2001, pp. 89 –95.

[12] Gokhale, S., Dasgupta, P., Distributed authentication for peer-to-peer networks**,** *Proceedings of Symposium on Applications and the Internet Workshops*, Jan. 2003, pp. 347 –353.

[13] Cahill, V., et al, Using trust for secure collaboration in uncertain environments, *Pervasive Computing, IEEE* , Vol. 2 Issue 3, July-Sept. 2003, pp. 52 –61.

[14] Li Xiong, Ling Liu, A reputation-based trust model for peer-to-peer e-commerce communities, *IEEE International Conference on E-Commerce*, June 2003, pp. 275 –284.

[15] Yao Wang, Vassileva, J., Trust and reputation model in peer-to-peer networks, *In Proceedings of Third International Conference on Peer-to-Peer Computing*, Sept. 2003, pp. 150 –158.

[16] Azzedin, F., Maheswaran, M., Trust modeling for peer-to-peer based computing systems, *Proceedings of Parallel and Distributed Processing Symposium*, April 2003, pp. 99 –108.

[17] Singh, A., Ling Liu, TrustMe: anonymous management of trust relationships in decentralized P2P systems, in Proceedings of *Third International Conference on Peer-to-Peer Computing*, Sept 2003, pp. 142 –149.

[18] Andrew “Bunnie” Huang, The Trusted OC: Skin-Deep Security, *Computer*, Oct. 2002 vol.35, no.10, pp.103-5.

[19] Yan, Z.; Cofta, P. Methodology to Bridge Different Domains of Trust in Mobile Communications, The First International Conference on Trust Management, Greece, May 2003.