[**Publication 4]** Zheng Yan and Piotr Cofta, "A Mechanism for Trust Sustainability among Trusted Computing Platforms", In *Proceedings of the 1st International Conference on Trust and Privacy in Digital Business (TrustBus2004)*, LNCS Vol. 3184/2004, pp. 11-19, Spain, September 2004.

http://www.springerlink.com/openurl.asp?genre=article&id=doi:10.1007/b99832

A Mechanism for Trust Sustainability among Trusted Computing Platforms

Zheng Yan[1], Piotr Cofta[2]

[1] Nokia Research Center, Nokia Group, Helsinki, Finland
zheng.z.yan@nokia.com
[2] Media Lab Europe. Dublin, Ireland
piotr.cofta@medialabeurope.org

Abstract. Trust plays an important role in social life as well as in cyberspace. Trust establishment in cyberspace relies on human beings as well as digital components. Trusted computing platform (TCP) was proposed to improve the trust between users and their devices. However, current TCP lacks solutions for trust sustainability among TCPs, so that trust relationship might be broken after a period of time. In order to solve this problem, this paper presents a mechanism for sustaining trust among TCPs. The mechanism builds up the trust relationship based on the root trust module (RTM) at a trustee and ensures the trust sustainability according to pre-defined conditions approved at the time of trust establishment and enforced through the use of the pre-attested RTM until the intended purpose is fulfilled. The paper also presents the applicability of the trust sustainability mechanism in several application areas.

1 Introduction

With the rapid growth of internetworking and electronic commerce, trust plays a crucial role in cyberspace in order to provide various digital services [1-3]. However, establishing trust relationship in cyberspace is more complicated than in social world. This is because communication in the cyberspace relies not only on human beings but also on digital components. Moreover, it is also more difficult to accumulate accurate information for trust purpose in remote digital communications. Generally, it is reasonably easy to initiate trust based on many existing technologies and structural regulations, but hard to sustain the trust during the fulfilment of the whole services.

Trust in digital information society, called digital trust, introduces two major challenges. The first one is to establish trust between users and their devices (e.g., PC and mobile phone) that is necessary to start the communication. With the increasing complexity of devices and various software running on the devices, it is very difficult for users to verify that their devices work properly. Trusted computing platform (TCP) has been proposed to solve the problem [7].

The other challenge is that the trust has to be sustained over time. For example, trustor A's trust on trustee B at one moment does not mean A could trust B at the next moment. The trust relationship built at the beginning of the communication should be maintained at least until the service is completed. It is essential to monitor and control

the conditions to sustain the trust for the final success of the service. This paper will mainly focus on solving the second challenge that has not been yet properly explored.

This paper mainly presents a mechanism for sustaining trust among TCPs. The mechanism can automatically inform the trustor about any distrustful behaviour of the trustee according to pre-defined conditions. Thereby, the original established trust relationship would be regulated accordingly. The paper contributes in three aspects. Firstly, issues for sustaining trust relationships are discussed. Secondly, a mechanism for trust sustainability is presented. Thirdly, the mechanism is applied for many real applications, e.g., MIDlet applications' trust on mobile information device (MID).

The rest of the paper is organized as follows. Section 2 presents related work. Section 3 describes the problem considered in the paper. Section 4 presents the trust sustainability mechanism and its applications are discussed in Section 5. The conclusions and future work are given in the last section.

2 Related Work

There is a large range of existing work on trust in information technology. The concept of trust is defined in various ways in the literature [1-3]. 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 dynamic as it is affected by many factors that are hard to monitor.

In order to figure out the trust in digital space, many people believe that some metrics should be defined to state various degree of trust [4]. A number of computational trust models were presented in [9-13]. These models compute the trust based on trustors direct or indirect experience. However, these models only pay attention to the influence of previous knowledge on the trust, but ignore future changes that may destroy the established trust. Thereby, it lacks support for cases that demand the trust for a longer period of time.

There is also a lot of work done on trust management [17-19]. Trust management systems provide trust assessments based on some trust root e.g. on policy assertion and trust specifications, which is also a major foundation of this paper as well.

Another important work in the literature is Digital Rights Management (DRM) [15]. It deals with client-side control of the usage of digital information. The trust model of traditional DRM solution can be described as a reference monitor (generally a software application) existing at a user's system for controlling usage of disseminated digital information in lieu of an information issuer. Not only DRM poses significant technical and operational challenges but none of existing DRM solutions considers how to sustain the trust relationship.

The paper is highly related to work on trusted computing platforms [5-8]. All work on TCP is based on the hardware security and cryptography to provide a root trust module at a digital computing platform. However, as described in next section, current work on TCP still lacks support on trust sustaining over the network. This is the key problem that the paper tries to solve. We believe trust management in the cyber-

space should be extended not only for trust assessment, but also for trust sustainability.

3 Problems with trust sustainability in TCP

The intention of this section is to clarify one of the problems of current TCP used for remote digital services. In TCP the trust is built upon a root trust, which is enforced by sound technologies, and realized through secure hardware [5, 6]. Every time a computer is reset, the root trust module steps in, checks itself, and then verifies the OS loader (e.g. BIOS) before letting the boot-up continue. Through checking the integrity metrics of different components, the OS loader is assumed to verify the operating system, then, the operating system is assumed to verify every piece of software, and so on. A remote computing platform can be trusted by challenging its integrity metrics, verifying and comparing them with expected values that represent components that are trusted enough to perform the intended purpose. If compared values match the expected values, trusted interaction with the remote computing platform can be commenced. Anomalous metrics indicate that the platform is not operating as expected and further communication with the platform should be reconsidered.

However, the trust in the remote platform (remote device) neither necessarily remain intact for an extended period of time, nor does it remain intact after hardware or software configuration changes. Actually, as the trusted remote computing platform is built up during system boot, the root trust module can only verify OS within the previously identified configurations, thus failing to verify the trust for any newly added hardware or software components. This also means that the trust on remote platform cannot be sustained even though the platform could have been trusted at some moment. Therefore, one disadvantage of the current TCP paradigm is that it does not provide a dynamic solution and is thus unable to sustain its protection in changeable environment.

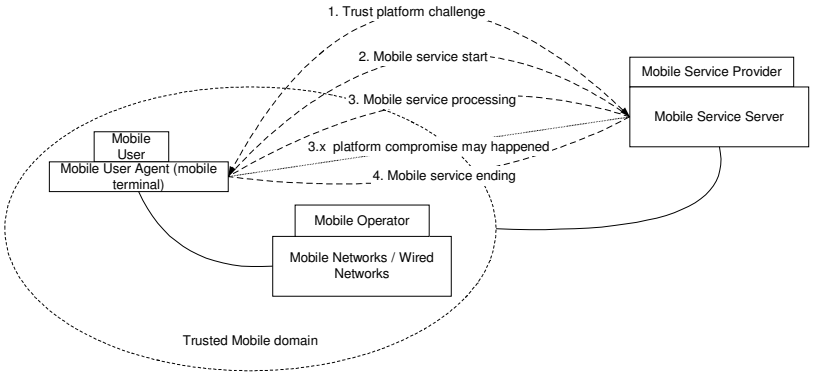

Fig. 1. An example of trust in mobile services

In order to illustrate the problem, we take mobile service as an example. The term 'mobile services' can be vaguely defined as services that are provided to mobile users via mobile terminals [16]. Specifically, mobile terminals such as mobile phones are considered to be the user agents of mobile services. As shown in Figure 1, a mobile phone already has the trust relationship with its operator through the existence of SIM (Subscriber Identity Module) and relevant authentication methods. A mobile service provider (SP) stays out of the usual trust relationship. Based on the TCP technology, it is possible for both the mobile SP server and the mobile terminal to verify each other as trusted computing platforms at the beginning of the service. However, as time passes, the SP server cannot guarantee that trust is sustained since hardware or malicious software can be installed in the mobile terminal

One simple solution is to periodically re-challenge the remote platform. This however requires frequent communication between the remote device and the server, the communication that is neither feasible nor economical in the mobile environment. Further, the remote device bears the burden of frequent and unnecessary computationally-intensive operations. Still, this method may be subject to some forms of the man-in-the-middle attacks.

4 Mechanism for trust sustainability in TCPs

In order to overcome the above problem, we introduce a mechanism for sustaining the trust among TCPs. We first present the trust formula used in the mechanism, and then the root trust module (RTM) on which the mechanism is based.

4.1 Trust form

The proposed mechanism uses the following trust formula: “Trustor A trusts trustee B for purpose P under condition C based on root trust R”. The difference between this formula and others is in the element C - conditions to trust. The element C is defined by A to identify the rules for sustaining the trust for purpose P, the conditions and methods to get signal of distrust behaviours, as well as the mechanism to restrict any changes at B that may influence the trust relationship. The root trust R is the foundation of A’s trust on B and its sustainability. Since A trusts B based on R, it is rational for A to sustain its trust on B based on R controlled by the conditions decided by A. This formula makes it possible to extend one-moment trust over the longer period of time.

4.2 Root trust module

The proposed mechanism is based on a root trust module (RTM), which is also the basis of TCP. The RTM could be an independent module embedded in the computing platform. It could also be a build-in feature in the current TCP’s Trusted Platform Module [6].

The root trust module at the trustee is most possibly a hardware security module that has capability to register, protect and manage the trust conditions, monitor any computing platform's change including any alteration or operation on hardware, software and their configurations, check changes and restrict them based on conditions, as well as notify the trustor accordingly. Herein, a trusted community refers to a trust relationship established between the trustor A and the trustee B and sustained for an intended purpose. Figure 2 illustrates a basic structure of this module.

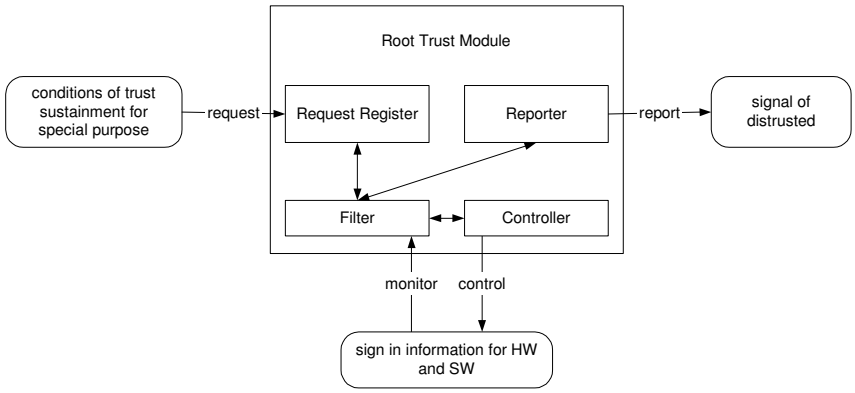

Fig. 2. Root trust module

4.3 Mechanism for trust sustainability

As postulated, the trust relationship is controlled through the conditions defined by the trustor, which are executed by the RTM at the trustee on which the trustor is willing to depend. The reasons for the trustor to depend on the RTM at the trustee can be various. Herein, we assume that the RTM at the trustee can be verified by the trustor as its expectation for some intended purpose and cannot be compromised by the trustee or other malicious entities later on. This assumption is based on the work done in industry and in academy [5-8].

As shown on Figure 3, the proposed mechanism comprises the following procedures.

a) Root trust challenge and attestation for ensuring the trustor's basic trust dependence at the trustee in steps 1- 2;
b) Trust establishment by specifying the trust conditions and registering them at the trustee's root trust module for the trust sustainability in steps 3-6;
c) Sustaining the trust relationship in the trust community through the root trust module monitor and control in steps 7-8;
d) Re-challenge the trust relationship if necessary when any changes against trust conditions are reported.

As it can be seen from the above protocol, the trust is based on the trustor's dependence on the RTM. Although the RTM is located at the trustee, its execution for trust maintenance and sustainability is based on the agreed conditions and rules approved by both the trustee and trustor at the time the trust is built.

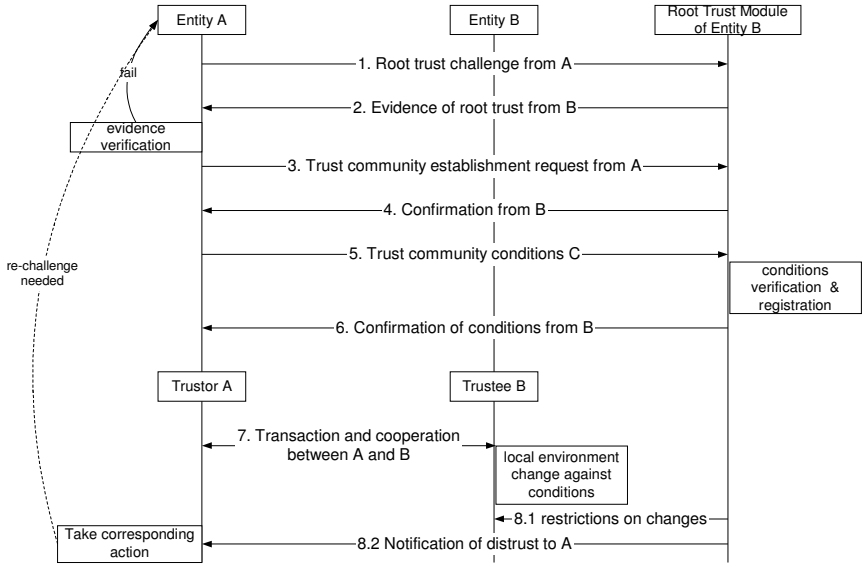

Fig. 3. Protocol for trust sustainability

5 Applications

The mechanism proposed above provides a way to sustain the trust. It can be used to support any services that are using remote digital communications. It could also be applied for building up personalized trusted computing platform. This section presents some of its applications.

5.1 Trusted MIDlet

One of the most popular mobile terminal applications is Java MIDP (Mobile Information Device Profile) application - MIDlet. There are certain measures to evaluate trust in MIDlets at the time they are loaded into the device. However as the MIDlet may be modified from its original state or illegally copied, its provider can no longer trust it after the installation. This introduces security problems in mobile services that interact through MIDlet with the service provider. Digital signatures and Digital Rights

Management (DRM) procedures are currently unable to solve all the problems successfully. As shown in Figure 4, the current MIDP 2.0 can support the trust attestation from MID (Mobile Information Device) to MIDlet, but lacks support on building up and sustaining the essential trust from the MIDlet or MIDlet providers to the MID running environment.

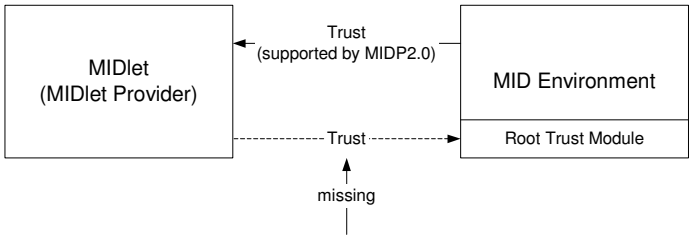

Fig. 4. One-way trust relationship between MID and MIDlet

With the proposed mechanism, the trust relationship could be sustained between a MIDlet provider (or a MIDlet) and a mobile information device. The method comprises attaching trust conditions to a MIDlet suite, downloading the MIDlet suite with attached trust conditions to the MID's RTM (already trusted by the MIDlet provider), checking the trust conditions against any alteration of the MID to determine a violation of the trust conditions and restrict changes accordingly, as well as reporting the violation to the MIDlet provider if necessary.

Complementary to DRM solutions that control the lifecycle of the MIDlet itself, this solution allows to express flexible rules associated with the execution environment of the MIDlet.

5.2 Personalised TCP

Current TCP technology forces users to accept pre-set rules defined by service providers, with no ability to personalise them according to their preferences. This kind of 'blind trust' is one of the biggest barriers that delays the acceptance of TCP, especially by end users. With the help of the proposed mechanism, the trust can be built according to the user's personalized conditions and based on the same root trust module already built into the digital device. In this case, the user is the trustor while the digital device is the trustee. The root trust module will behave as a crucial component in the future TCP compliant devices. It will inform the user about any distrustful behaviour of the device or restrict some changes at the device according to the user's personal trust specifications. Potentially such mechanism may alleviate also some of the privacy issues commonly associated with TCP.

5.3 Trusted ad hoc networking

A mobile ad hoc network (MANET) is a collection of autonomous nodes or terminals that communicate with each other over relatively bandwidth-constrained wireless links. It is a new paradigm of networks where all network activities including discovery of the topology and delivery of messages must be executed by the terminals themselves. The MANETs are generally more prone to physical security threats, such as eavesdropping, spoofing, denial-of-service, and impersonation attacks.

With the proposed mechanism embedded into the ad hoc network terminals, it is possible for those devices to build the trusted community for autonomous communications. The trusted community is composed of a number of nodes following a common intended purpose, as shown in Figure 5. By imposing identical trust conditions on members of the community the required trusted behaviour could be assured.

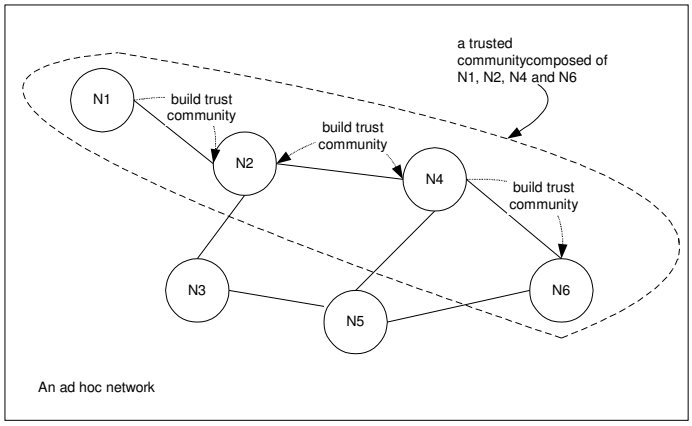

Fig. 5. Establishing trusted community in ad hoc networks

5.4 VPN trust management

Trust plays a key role in the context of virtual private networking (VPN). However, providing advanced trust into VPN networks has proven to be problematic as none of existing VPN systems can ensure that data or components on a remote user terminal can be controlled according to the VPN operator's security requirements even though the user verification is successful, especially during the VPN connection and after disconnection. Nowadays, the VPN operators depend on user's responsibility to address this potential security problem.

The proposed mechanism provides a solution for the above problems. In this case, a VPN management server is the trustor, while VPN a client terminal is the trustee. The VPN management server identifies the client terminal and specifies the trust conditions for that type of terminal at the VPN connection. Thereby, the VPN client terminal could behave according to the VPN operator's expectation.

7 Conclusions and Future Work

This paper presented a mechanism to sustain the trust among TCPs on the base of the root trust. The formula of trust used throughout this paper takes on the form "A trusts B for P under C based on R". The formula creates the trust based on the attestation of the RTM at the trustee and controls its sustainability according to the pre-defined conditions C. Those conditions are approved by both the trustor and the trustee at the time of trust establishment and enforced through the use of the pre-attested RTM until the intended purpose is fulfilled.

The paper extends the trust model from static to dynamic. Thus, it develops the notion of using trust management not only for the trust assessment but also for the trust sustainability. The proposed mechanism could be applied in many real applications for the trusted services and communications. It could work as an extension of future trusted computing platform to support various applications with greater flexibility.

Our future work will focus on developing the theory of trust model and prototyping the mechanism for trusted mobile Java applications.

References

1. Kari Chopra, William A. Wallace: Trust in Electronic Environments. Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03), 2003.
2. McKnight, D. Harrison, Chervany Norman L.: The meanings of Trust. UMN university report. 2003.
3. 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).
4. Peter Herrmann: Trust-Based Protection of Software Component users and Designers. In Proceedings of the First International Conference of Trust Management (iTrust 2003), Crete, Greece, May 2003.
5. Davis P T, TCPA: who can you trust. EDPACS: the EDP Audit, Control and Security Newsletter, Dec. 2002.
6. Vaughan-Nichols, S.J., How trustworthy is trusted computing? Computer, Volume 36, Issue 3, March 2003.
7. Paul England, Butler Lampson, John Manferdelli, Marcus Peinado, Bryan Willman: A Trusted Open Platform. IEEE Computer Scciety, p55-62, July 2003.
8. Adrian Baldwin, Simon Shiu: Hardware Security Appliances for Trust. In Proceedings of the First International Conference of Trust Management (iTrust 2003), Crete, Greece, May 2003.
9. Daniel W. Manchala: Xerox Research and Technology. E-Commerce Trust Metrics and Models. IEEE Internet Computing, vol.4, no.2 p.36-44 (2000).
10. 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.
11. A. Jøsang and S. J. Knapskog: A metric for trusted systems. In Proceedings of the 21st National Security Conference, NSA 1998.
12. A. Jøsang: An Algebra for Assessing Trust in Certification Chains. In J.Kochmar, editor, Proceedings of the Network and Distributed Systems Security (NDSS'99) Symposium, The Internet Society, 1999.

13.A. Jøsang: A Logic for Uncertain Probabilities. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems. 9(3), pp.279-311, June 2001.
14.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.
15.Jaehong Park, Ravi Sandhu: Towards usage control models: beyond traditional access control. Proceedings of the seventh ACM symposium on Access control models and technologies, Monterey, California, USA, 2002.
16.Zheng Yan, Piotr Cofta: Methodology to Bridge Different Domains of Trust in Mobile Communications. The First International Conference on Trust Management (iTrust2003), Crete, Greece, May 2003.
17.A. Jøsang, N. Tran: Trust Management for E-Commerce. In proceedings Virtual Banking 2000. DSTC university report, 2003.
18.Matt Blaze, John Ioannidis, Angelos D. Keromytis: Experience with the KeyNote Trust Management System: Applications and Future Directions. In Proceedings of the First International Conference of Trust Management (iTrust 2003), Crete, Greece, May 2003.
19.Tyrone Grandison, Morris Sloman: Trust Management Tools for Internet Applications. In Proceedings of the First International Conference of Trust Management (iTrust 2003), Crete, Greece, May 2003.
20.Felten, E.W.: Understanding trusted computing: will its benefits outweigh its drawbacks? IEEE Security & Privacy (May-June 2003) vol.1, no.3, p.60-2.