[MGAMSt04] Ivan Martinovic, Manuel Goertz, Ralf Ackermann, Andreas Mautne Ralf Steinmetz **Trust and Context: Two Complementary Concepts for Creating Spontaneous Collaborative Networks and Intelligent Applications;** International Conference on Software, Telecommunications and Computer Networks SoftCOM, Split, Oktober 2004. S.

Trust and Context: Complementary Concepts for Creating Spontaneous Networks and Intelligent Applications

Ivan Martinovic, Manuel Görtz, Ralf Ackermann, Andreas Mauthe, Ralf Steinmetz
Multimedia Communications Lab
Department of Electrical Engineering and Information Technology
Darmstadt University of Technology
Member of E-Finance Lab, Frankfurt am Main
{Ivan.Martinovic, Manuel.Goertz, Ralf.Ackermann, Andreas.Mauthe, Ralf.Steinmetz}@KOM.tu-darmstadt.de

***Abstract*— A realistic future scenario comprises almost ubiquitous network access. Nevertheless, such connectivity may not necessarily fulfill every user's needs or it could even overload a user by irrelevant information. The key issues in appropriate adaptation of services to suite the user is the context awareness. It includes the reasoning about the environment and its influencing factors. In this paper we present ideas and discuss the procedures in providing adaptive levels of trustworthiness depending on different user's tasks in different environments. The objective of this paper is to describe the fundamental concepts of trust and context and how they add value to each other. Furthermore, we discuss possible scenarios where context can be used as a parameter for defining trust and also where trust can be used to support a secure sharing of context information between various entities involved.**

1. MOTIVATION

The way in which people use computers has changed dramatically over the past decades. At the dawn of the computer era many people shared a single large computer (mainframe). However, with introduction of the personal computer the view has changed. Each individual uses a single computer that suites its personal purposes. In recent years the relationship between humans and computers has changed into a one-to many relation. One user now has a multitude of computing devices at hand. These devices such as cellular phones for audio communication or electronic calendars for storing addresses and dates are typically specialized for distinct purposes. The Weiser's description of ubiquitous and pervasive computing and the era of "calm technology" is starting to be a part of our everyday life [1].

In our vision of the near future networks will become more intelligent by being able to sense and consider the context of communication and the knowledge of a community of nodes. These networks will have distributed and decentralized nature of various heterogeneous and autonomous nodes, which pose many challenges where the traditional network concepts with central authorities and a-priori existing infrastructures cannot directly be applied. Nodes will be able to establish relationships based on trustworthiness to increase protection of their privacy but also to enhance the performance of different tasks.

1.1 Related Work

Research of decentralized, heterogeneous systems have been widely investigated over the last decade. The growing importance of seamless communication and increased use of wireless technologies rise questions especially in the area of security and trustworthiness of communicating entities. Traditional security paradigms (mostly based on cryptographic mechanisms) do not provide the "silver-bullet" solution as their assumption on existence of central trusted authorities cannot always be met [2]. It is required to understand the trustworthiness of the entities by not only their identity but also their behavior. There is already a well-established research community dealing with a number of trust issues. One important area of research is the nature of trust by means of transitivity. While some researchers define trust as transitive, others consider transitivity to be more of a delegation of rights and that the transitivity should not be applied [3]. Nevertheless, the transitive characteristics of trust have already been used to extend security concepts such as the PGP scheme [4]. The PGP uses transitive closure to create the "web-of-trust" model and by allowing users to sign each others public key, they increasingly validate its trustworthiness and create a decentralized public key authentication chain. Another important aspect of trust is its formal definition. Analogically to a real world, trust has a subjective nature and depends on the context of a certain task and knowledge which in most cases is uncertain. In [5] the formal model for uncertain probabilities called subjective logic is described. It can be applied to define the subjective trust beliefs based on opinions and it provides more flexibility than binary logic. In [6] an implemented trust management system KeyNote is presented, it defines the authorization of different public keys, verification and policy assertions. The further work on terminology and definitions of trust, key management and trust based policies definition are well summarized in [7]. Concepts of trust have also been increasingly used as a part of cooperation incentives in the peer-to-peer systems where the trust based on reputation and credibility concepts can be used to identify non-cooperative nodes (e.g. free-riders) [8]. Similary, the topic of trustworthiness is considered to be more essential part for facilitating cooperation between the entities for dependable routing [9].

The objective of this paper is to describe the fundamental concepts of trust and context and how they add value to each other. Two representative scenarios are used to illustrate the benefits of the proposed approach. The rest of the paper is structured as follows: Section 2 describes the necessary concepts and definitions needed in the area of trust and context. In addition, we show the influence of context on trust and vice versa. In Section 3 we establish common scenarios and practical contribution of usage. Section 4 covers potential future work and further challenges.

2. CONCEPTS & DEFINITIONS

2.1 Context

The usage of context information is an enabling technology for a large variety of applications. Most of these applications try to dis-burden the user from re-occurring tasks that are not central, but only influence (e.g. parameterize) communication tasks. It is an important characteristic of context-aware applications that they are explicitly meant to disappear from the users perception.

1) Context Definition: The term *context* is widely used and most people have a general idea about what context is. However, it is used with very different meanings and there are diverse (and often vague) notions about what the term actually describes. A very generic definition can be found in [10]:

> Context: That which surrounds, and gives meaning to something else.

However, the definition is too general for the purpose of building context-aware and ad-hoc applications. The analysis of other computing science areas leads to the conclusion that context is widely used with different meanings. In the area of artificial intelligence contexts are abstract objects in a domain and statements can be made "about" them [11]. McCarthy [12] states that the main question of *what context is* cannot be answered as a result of a unique conclusion. Instead, various notions of context each for its application will be found useful.

Applications are context-aware if they use context to provide relevant information and services to the user, where the relevancy depends on the users task [13]. Main usage scenarios of context in such applications have been identified in [14]. These applications automatically *adapt* their behavior according to discovered context (using active context), or *present* the context to the user using reductions of all possible information and *store* the context for the user to retrieve later (using passive context).

2) Context Usage: The utilization of context information requires several processing steps. Typically, the following steps can be identified: *acquisition*, *synthesis*, *dissemination* and *use*. The resulting abstract procedure is described in the *context cycle* shown in Figure 1. The Context Cycle model follows the principle of the Omnibus Model for multi-sensor fusion [15].

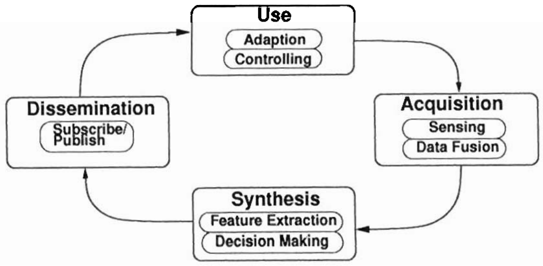


Figure 1 – The Context Cycle

The automatic acquisition of context information is a prerequisite to capture date from and model real world situations. A common way is the utilization of a multitude of sensors. Sensors are used to observe the physical world.

> A *sensor* is a device that perceives a physical property. It transmits the result of a measurement.
> A sensor maps the value of some environmental attribute to a quantitative measurement.

Two types of sensors can be distinguished [16]. *Physical sensors* are hardware components that measure parameters in the environment. They provide the information on electronic level, typically as analog output or as digital signals. *Logical sensors* are components that provide (aggregated or transformed) information that is not directly taken from the environment but represents information about the observed world. Information sources can be a clock as a sensor that offers time and a server offering the current exchange rate. Logical sensors supply the information most often as digital signal over a common interface such as a serial data connection or an HTTP-connection.

Each sensor S can be seen as a time dependent function that provides the system with a set of values which give a description of the context at a specific time. The function $S\colon t \rightarrow X$ returns a scalar, vector, or a symbolic value (X) [17]. The output of a single sensor might not produce sufficient information. The concept of *sensor fusion* describes the combination of sensory data or information derived from sensory data.

The context synthesis process assesses significant features of the context. This process uses the sensor information as an input and creates an abstract representation of the captured situation. Location, entity activity and time are typical context sources and form the *primary context*.

Knowledge of the current location and time together with a user's calendar lets an application have a good estimation of the user's current situation. It is preferable that the user's context is detected automatically. Finally, the context information has to be disseminated to a context consumer which stores or uses the information. The application uses the context information as an implicit input for e.g. parametrization of functional blocks, simplification of human computer interaction (HCI) and overall task automatisation. A multitude of context information sources, can mutually transmit their data. Typical context information sources are devices, such as Bluetooth sender, RF/IR-Badges or iCalendar-compliant applications [18].

2.2 Trust

The main difference between trust and traditional security is that trust does not only encompass (strong cryptographic) identity authentication and communication security but considers especially the behavior and relationships between entities. The dynamic nature of trust relationships can thus increase and decrease over time, which forms the basis for extended mechanisms to increase overall dependability of different systems. This allows to support dynamic and adaptable concepts. In this work we tackle a challenging approach to the usage of trust as a complementary concept for context-aware computing. We use trust to enable a better adaptivity to a different context data and more efficient synthesis of environmental knowledge. As already mentioned in Section 1, there is a expansive research about trust and its application. The related work cover many different aspects of trust, however there is no unified, well established definition.

We use the general definition of *trust* [19]:

> *Trust*: Confidence in or reliance on some quality or attribute of a person or thing, or the truth of a statement

In a more technical context, we choose the definition of [20]:

> *Trust*: Extend to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible.

This definition implicitly shows that trust depends on uncertain knowledge of dependability, risk assessment and awareness of the situation, which we consider to be the context. Also, other parts of this concept are the entities *trustor* and *trustee*, which are defined as:

> *Trustor*: The entity who has a certain level of trust in another entity (being subject).
>
> *Trustee*: The entity who is being trusted, or to whom something is entrusted [19]; a person in whom confidence is put (being object).

The main characteristics of a trust relationship are:

- Subjective: A has a subjective opinion on the trustworthiness of B which depends on a specific *task* in a given *context* .
- Asymmetric: If A trusts B, it does not necessarily mean that B trusts A.
- Gradual: Different trust levels between entities can be defined e.g. similar to [4]: *Ultimately*, *Completely*, *Marginally* and an explicit negative trust*((Distrust)*.
- Transitive: If A trusts B and B trusts C, there is a certain level of trust between A and C.

The relationship between entities can be based on *direct* or *indirect* trust. We define a *direct* trust as:

> Trust relationship between trustor and trustee based on an evidence obtained by direct observation, experience or a prior configuration.

On the other hand, we define an *indirect* trust as:

> Trust relationship between trustor and trustee based on the transitivity and gradual nature of trust.

1) Building Trust: Building trust is a process which involves the acquisition of *trust evidence* which increases knowledge of the trustor and creates a belief in the trustworthiness of the trustee. The evidence can be based on identity trust which can be provided by cryptographic mechanisms like digital certificates, challenge-response protocols or any other authentication proof. In addition, it may be based on behavioral trust, which is especially interesting in environments where no centralized Public Key Infrastructure (PKI) exists and the identities of participants are unknown. In this case, the trust evidence is based on direct experience between trustor and trustee or indirect experience based on information reported from other entities.

2) Credibility: Credibility is the subjective opinion based on the given trust evidence and knowledge of the trustor. Every trustor can decide how important the given evidence is in a certain context. While digital certificates signed by trusted third party state the authentication of one's identity, it does not make any statement about its behavior. Thus, depending on the context and nature of a task, the credibility of the same evidence may vary e.g. participants of an on-line auction system base the seller's trustworthiness on his behavior, while by on-line banking the identity of the bank's web site is crucial for the secure transaction.

3) Risk Threshold: This parameter defines the quantity of the evidence required to build a particular trust relationship. We define the *Risk Threshold* as a function of knowledge about the context and subjective estimation of an importance of a task.

> Risk Threshold := *knowledge of (infrastructure parameters, risk paramterers)*

Here the *infrastructure-parameters* denote the characterization of a context e.g. security mechanisms like PKI to ensure end-to-end security, but also the visual contact or possibility for direct checking of one's public key fingerprints with communicating persons. The *risk parameters* refer to various hazards and the different threat models possible in an certain environments.

Figure 2 shows a summary of trust terminology described in this section. The trustee provides the trust credential to a trustor, who then weights that credential with the credibility of the trustee. The risk threshold defines the measure of the quantity of trust credentials which is required to establish certain trust relationship. The risk threshold also depends on the context in which this trust should be provided.

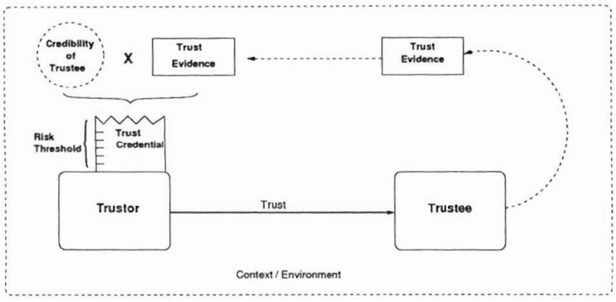


Figure 2 – Building Trust

3. SCENARIOS

The following scenarios are used to motivate and illustrate the proposed approach in this paper. One scenario describes the utilization of context information as a trust parameter. The second scenario shows how to use trust in a context sharing application.

3.1 Context as Parameter for Trust

In order to show how the Risk Threshold can be modeled as a context-dependent metric, we present a typical collaboration scenario. Figure 3 describes different scenarios within the context's dimensions of *environment openness* and *network dynamics*. Environment openness is the measure for existence of infrastructure, services provided within that infrastructure, and given credibility of those services. The network dynamics denote a parameter of user dynamics. It can be derived from user mobility, network consistency (link stability), and the number of users who are already known or unknown. In such different scenarios the question could be: "How trusted is the execution of a certain task in a given environment?". Here the Risk Threshold represents a trade-off between the security requirements to create trust relationships (e.g. risk assignment) and the performance of creating such relationships.

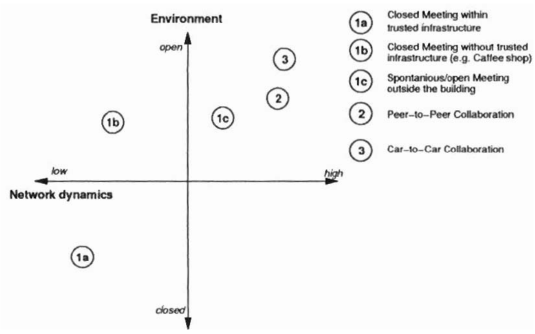
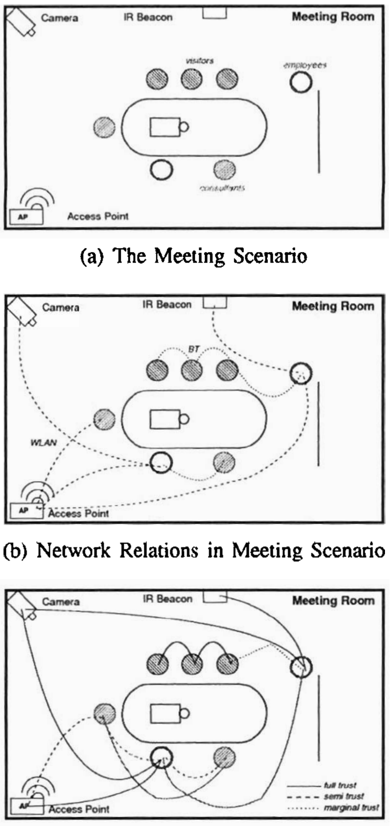

Environment
open
closed
low
high
Network dynamics
1a
1b
1c
2
3
1a Closed Meeting within trusted infrastructure
1b Closed Meeting without trusted infrastructure (e.g. Caffee shop)
1c Spontanious/open Meeting outside the building
2 Peer-to-Peer Collaboration
3 Car-to-Car Collaboration

Figure 3 – Dimensions of context and different scenarios

The scenario denoted in 1a is a typical business meeting scenario where participants are all members of the same corporation. They form a closed group of participants. Even a passive attack (e.g. eavesdropping) can be avoided by the utilization of trusted infrastructure which provids appropriate cryptographic services. The Risk Threshold in this scenario can be higher, because enough security guarantees can be assured by infrastructure which is a-priori trusted. Furthermore, the risk parameters, which in this case are formed by the participants, will already have a certain trust degree between each other as they are all part of the same trust domain (in this case corporation). The Scenario 1b is analog to 1a, however the meeting takes place within an untrusted infrastructure (e.g. coffee shop). The participants can also be from different trust domains (e.g. different corporations), but not-trusted infrastructure is still sufficient for providing services for establishing an end-to-end security for communication between the trustor and trustee by the usage of digital certificates. In this scenario, the Risk Threshold should be lower as the trustor requires more information about the trustee. On the other hand, in scenario 1c no infrastructure exists. The meeting is a spontaneous network of different participants and they need to cooperate to establish a trusted network for communication. This scenario is common for ad hoc networks. The network dynamic increases as there might not be explicit differences between participants and non-participants. The increased possibility of active or passive attacks exist, thus the risk threshold is even lower. The only advantage that still can guarantee certain a-priori trust is a visual contact between the participants, which can help to establish a direct and secure communication by e.g. Infrared (IR) Beacon. Scenario 2 depicts a popular P2P file sharing scenario which can also be seen as a spontaneous collaborative network. The participants are commonly unknown to each other and the network dynamic is high due to uncontrollable users connections and disconnections. For the reason of the very high number of users and its decentralized nature, the infrastructure of such systems is not common. The trust building process of such scenarios incorporate direct and indirect trust techniques, while risk threshold strongly depends on the task and the knowledge of the trustor.

3.2 Trust as Parameter for Context Sharing

Figure 4(a) shows a set of different entities in the same environment. The entities are attendees of a meeting containing heterogeneous devices (e.g. PC, PDAs, mobile phone) with different connections to a diversity of sensors (e.g. WLAN Access Points, Cameras, InfraRed Beacon, Bluetooth). They all create network relations by their point-to-point communication as shown in Figure 4(b). These network relations provide the underlying basis for creating an overlay trusted network, that is based on the trust building concept. In this case the trust evidences can be aggregated from different participants and different sensors e.g. a trust evidence could be a membership of the same WLAN group defined by sharing a same WEP key, or having a paired Bluetooth devices. Participants from different trust domains, may also set different risk thresholds in this environment. Their trust relationships between other participants and sensors will vary as shown in Figure 4(c). This relationships will then be used to share the context information



(a) The Meeting Scenario

(b) Network Relations in Meeting Scenario

(c) Trust Relations in Meeting Scenario

Figure 4 – Relationship of Context, Network and Trust

between participants according to the user's preferences and it's privacy policies.

Even among trusted users the type of information may vary according to the user's polices. Therefore, different levels of details are needed for appropriate sharing of the context. These levels can then be mapped to specific persons or groups. In an given example the fact of being in a meeting can be shared with the requestor using e.g. a three level model as follows:

- Level of Detail 1: out of the office
- Level of Detail 2: in a meeting
- Level of Detail 3: in a meeting from 1:00 pm to 3:00 pm in room 348

4. CONCLUSION AND OUTLOOK

The goal of this work was to present a new facet in the research of context-awareness and trust. This document is based on our current research. We use the notion of trust to enhance collaboration between participants in different situations and to increase the user's trust in tasks depending on different contexts. The presented definitions and concepts of trust and context show their emergence as an important aspect for the creation of spontaneous networks and intelligent applications, respectively.

In our future work we will concentrate on formalizing the risk in different environments to automatically determine the Risk Threshold and requirements on trustworthiness to match different threat models. The investigation of different security mechanisms and their mapping onto different trust policies should help us to define valid trust credentials which then need to be requested for appropriate trust relationships.

Another important research aspect is the further investigation of trust as a quantifiable metric. This metric can be used for defining and measuring reliability, dependability and confidence of an entity or a system. Trust then can be used as a part of a Service Level Agreements (SLAs) to assure a certain level of quality of service and to support different technologies e.g. Web Services.

REFERENCES

[1] M. Weiser, "The computer for the twenty-first century," *Scientific American*, vol. 265, no. 3, Sept. 1991.

[2] B. Schneier, *Secrets and Lies - Digital Security in a Networked World.* John Wiley and Sons, 2000.

[3] http://www.sandelman.ottawa.on.ca/spki/html/1997/spring/msg00346.html, "Discussion on transitivity of trust in the context of spki (simple pki)," 1997.

[4] P. Zimmermann, *The Official PGP User's Guide.* MIT Press, 1995.

[5] A. Josang, "A logic for uncertain probablilites," *Internation Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, pp. 279–311, 2001.

[6] M. Blaze, J. Feigenbaum, and A. D. Keromytis, "Keynote: Trust management for public-key infrastructures," in *Security Protocols Workshop*, May 1998.

[7] T. Grandison and M. Sloman, "A survey of trust in internet applications," in *IEEE Communications Surveys and Tutorials*, Forth Quarter 2000.

[8] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *International WWW Conference*, Budapest, Hungary, 2003.

[9] M. Hollick, I. Martinovic, T. Krop, and I. Rimac, "A survey on dependable routing in sensor networks, ad hoc networks, and cellular networks," in *Proc. EUROMICRO 2004*, Rennes, France, August 2004, accepted for publication.

[10] "On-line dictionary," http://foldoc.doc.ic.ac.uk/foldoc/).

[11] R. Guha, "Contexts: A Formalization and Some Applications," Ph.D. dissertation, Stanford, 1991.

[12] J. McCarthy and S. Buvač, "Formalizing Context (Expanded Notes)," *Computing Natural Language*, 1997.

[13] A. K. Dey, "Context-aware computing: The cyberdesk project," in *AAAI 1998 Spring Symposium on Intelligent Environments.* Palo Alto, CA: AAAI Press, March 1998, pp. 51–54, http://www.cc.gatech.edu/fce/cyberdesk/pubs/AAAI98/AAAI98.html.

[14] G. Chen and D. Kotz, "A survey of context-aware mobile computing research," Dept. of Computer Science, Dartmouth College, Tech. Rep. TR2000-381, November 2000. [Online]. Available: ftp://ftp.cs.dartmouth.edu/TR/TR2000-381.ps.Z

[15] M. Bedworth and J. O'Brien, "The omnibus model: A new architecture for data fusion?" in *Proceedings of the 2nd International Conference on Information Fusion (FUSION'99)*, Helsinki, Finnland, July 1999.

[16] A. Schmidt, M. Beigl, and H.-W. Gellersen, "There is more to context than location," *Computers and Graphics*, vol. 23, no. 6, pp. 893–901, 1999. [Online]. Available: citeseer.nj.nec.com/schmidt98there.html

[17] R. R. Brooks and S. Iyengar, *Multi-Sensor Fusion: Fundamentals and Applications.* New Jersey: Prentice Hall, 1998.

[18] M. Goertz, R. Ackermann, and R. Steinmetz, "Enhanced sip communication services by context sharing," in *Proceedings of the 30th EUROMICRO Conference*, August 2004.

[19] "Online oxford dictionary."

[20] A. Jøsang and S. L. Presti, "Analysing the relationship between risk and trust," in *In T. Dimitrakos (editor) the Proceedings of the Second International Conference on Trust Management*, April 2004.