A TRUST BASED DELEGATION SYSTEM FOR MANAGING ACCESS CONTROL

Rainer Steffen, Rudi Knorr*

Abstract

Trust is considered to be a powerful approach for managing access control in pervasive computing scenarios. We introduce a novel delegation system that describes digital trust between users by means of cryptographically secured tokens. The delegation system is organized by the users themselves in a fully distributed manner. A central instance like a public key infrastructure is not required. The system supports anonymity, provides a high usability and is suitable for use within pervasive computing scenarios.

1. Introduction

Security management in pervasive computing scenarios is a challenging task. We have to cope with dynamic and heterogeneous networks, a large number of different devices, users and services. To enable a secure collaboration between all the actors, an efficient access control is essential. In traditional computer and communication networks, access control is mostly managed by static access control lists (ACLs). These ACLs contain information about the objects that have to be protected (e.g. data files or services) and the subjects (e.g. users) which have the right to access these objects. Management of access control by ACLs presumes that the objects have knowledge about all the potential subjects, which might access the object.

In future pervasive scenarios, this kind of access control mechanism is unsuitable. Firstly the administrative overhead for managing the ACLs in a dynamic scenario with a multitude of devices, users and services is increasing tremendously. Secondly there is no support of unknown devices and users as they can appear in pervasive and ad-hoc networks. A powerful approach to overcome these problems is delivered by the trust-paradigm. Instead of or in addition to an inflexible ACL configuration, trust relationships between the users are utilized to gain access to the objects. The goal is to map the natural trust between humans to the digital world.

One of the trust approaches is the so-called delegation system which enables users to express and enforce the trust they have in others by means of digital trust tokens. In the following we elaborate a novel and user-friendly trust based delegation system that is suitable for the use within pervasive computing scenarios.

This paper is organized as follows: section 2 gives a brief overview of related work, section 3 presents the novel architecture and some implementation aspects and chapter 4 provides the final conclusion and outlook.

* Fraunhofer Institute for Communication Systems, Hansastrasse 32, 80686 Munich, Germany
{Rainer.Steffen, Rudi.Knorr}@esk.fraunhofer.de

2. Related Work

Digital Trust has become a widely accepted research field in the last few years. The intended field of applications comprises trust in very different areas. Examples are managing access control by using trust, trust for collaboration in (virtual) organizations and communities, estimation of trustworthiness of information and users, trust for electronic commerce and others. General overviews and surveys about trust in digital networks can be found in [2], [5] and [7]. When we consider trust as a mechanism for managing access control, the concept of trust based delegation systems is one approach.

The basic idea behind delegation systems is that some active entity in a system delegates authority to another active entity in order to carry out some functions [1]. Depending on the design, delegation can be performed at a central instance (e.g. server) or in a decentralized manner using tokens or tickets to describe the delegation process. Usually tickets describe an operation that can be carried out by owning or delivering the ticket (e.g. access to an event or paying an amount of money). A ticket is issued exclusively; it can be passed on to someone else but can not be duplicated. Exemplary ticketing systems are described in [3] and [4]. Tokens resemble tickets, with the difference that tokens can be duplicated and the effect of tokens can be restricted. The delegation of access rights with tokens can be based on trust relationships between users. Such a trust based delegation system is introduced in [6], at which the propagation of tokens and thus the access rights depend on the trust the users have into each other.

Using trust based delegation systems for managing access control in pervasive environments is an attractive and feasible method. The main problem of the known trust based delegation systems is that they depend on a public key infrastructure (PKI). A central PKI is in conflict with the mainly decentralized character of pervasive and ubiquitous systems. A PKI always requires authentication, thus all the potential users of the system must be known by the PKI; ad-hoc connections with unknown users and devices are not supported. The need of a PKI also implies that an offline-delegation outside the system is not possible.

In the following, we present a new and feasible trust based delegation system that overcomes the described problems.

3. Architecture of the Trust Based Delegation System

The purpose of the described trust based delegation system is to use natural trust relationships to gain access to digital services. We assume that every digital resource or object can be modeled as a service with an access control entity and a service invocation method.

Fig. 1 shows the basic principle of that concept. A trust source generates a token with explicit information about the access rights to a specific service or a trust value that describes the trust relationship between the trust source and user A. A trust value is described by a defined metric and can be seen as a kind of reference or attestation. User A can pass a copy of the token on to user B with the option to modify the access rights or the trust value in dependence on the trust user A has in user B. User B can act in the same way and distribute the token to another user he trusts. The token propagation, the permissions and trust values map the natural trust between the users into the digital world.

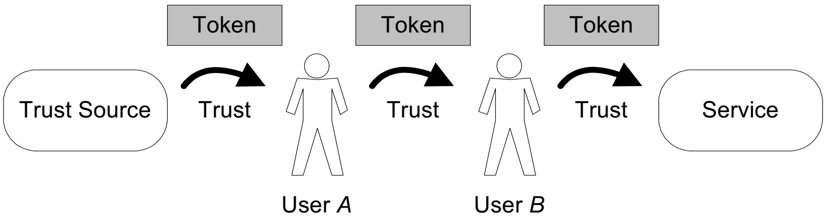

Figure 1: Trust chain

During the service invocation user *B* delivers the token to the service. Through the content of the token, the service decides autonomously if the access will be granted or not. To some extent this approach is similar to a ticketing system, with the difference that we can copy and restrict our tokens. Our architecture allows an anonymous propagation of tokens without the need of a PKI, which is a novelty.

Trust always implies uncertainty, thus risk has to be taken to a certain extent that a user acts different from what we would expect. In contrast to conventional access control systems like ACL, trust can only provide soft-security. Such a trust based access control system is appropriate to secure objects that have a small value and the demand for an easy to use access control.

3.1 Securing the Tokens

A token is an electronic information that comprises access permissions and trust values (in the following referred to as permissions). The permissions can be coupled to constraints like location, time, or in general, context. For example, a token can have a valid permission for a specific time of day or while the token holder acts in a specific surrounding. The tokens are described using the extensible markup language (XML) and can be transferred over arbitrary networks.

The trust source is responsible to create an initial token that comprises a digital secret. This secret is only known to the trust source and the service the token is appointed to. The trust source and the service can be the same physical device. In a ubiquitous office scenario, for example, the trust source could be the administrative department or a system administrator. Every time a new token is generated by the trust source, it creates a new digital secret.

In addition to the secret the token contains a public key (pub) for asymmetric encryption. The associated private key is only known by the service. The secret as well as the current permissions and constraints are stored inside the token as encrypted values; plaintext information about the current permissions is also enclosed so that the user can examine it. Fig. 2 a) shows an exemplary token for a first user (user *A*).

User *A* can decrease the permissions and modify the coupled constraints before he gives an instance of the token to the next user (user *B*). User *A* encrypts the new permissions, along with the already encrypted part of the token, using the public key (Fig. 2 b). Again the current permissions are stored in plaintext inside the token. User *B* and the following users can act in the same way.

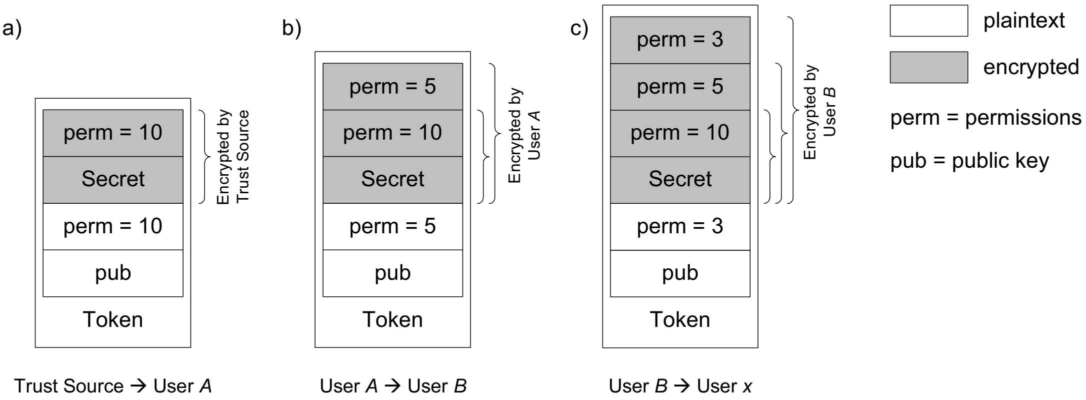

Figure 2: Multiple encrypted token

When a user wants to invoke a service, he delivers the token to the service that has to decipher the encrypted part of the token recursively with the private key until the primary secret is visible in plaintext. While deciphering, the integrity of the token is checked; illegal changes can easily be identified and if needed, the token can be blocked. On the basis of the last permissions, the service can decide itself whether to grant access or not. Since the integrity of the complete trust chain - from the trust source to the service - is secured by cryptographic measures, there is no need for a PKI and user authentication. Thus, also unknown users and devices can be supported.

If a token is copied illegally (e.g. stolen from a user) or the trust between two users is broken, a revocation token can be used to annul or limit the permissions. For this reason an optional permission update list can be established inside the service. Every time the service decrypts an instance of the token, it checks the permission update list for current changes and uses the potential revocation token accordingly.

3.2 Implementation

The described trust based delegation system was realized as a demonstrator. The software to manage the tokens (receive, relay and restrict) was implemented in Java on Windows Pocket PC handhelds. An exemplary service (light control) and the token based access control mechanism were implemented on a standard PC. The demonstrator offers a graphical user interface to easily exchange tokens between the handhelds by using wireless LAN. Owners of valid tokens are able to invoke the exemplary service and control the lighting according to the received permissions. Preliminary tests show that the system provides a high usability and user convenience. The effort to encrypt the tokens inside the handhelds and to multiply decrypt the tokens inside the access control entity of the service is quite low, so that no noticeable delays can be experienced.

In the future, this demonstrator will be extended to support additional services provided by a service management middleware. Planned services are amongst others a trust based web site access, the support of electronic lock systems and the control of wireless LAN internet access for visitors. As the client software is written in Java it can quickly be ported to other platforms (e.g. PCs or mobile phones) and can easily be installed on different devices.

4. Conclusion and Outlook

In some scenarios ease of use is valued more than the value of the objects that have to be protected. This occurs especially in pervasive scenarios, where usability is the key factor to user acceptance and often the objects to be secured are of small value.

The presented delegation system allows a secure and easy to use trust based access control mechanism for pervasive scenarios. The described architecture allows an anonymous propagation of tokens without the need of a public key infrastructure, which is a novelty. The user is not confronted with authentication, tokens can be passed on even if communication with the system itself is not possible (offline delegation) and unknown users and devices are supported. Permissions of a token can be restricted and the integrity of the trust chain can be checked by cryptographic measures. To increase the controllability of the system and to motivate users not to abuse the trust someone gave them, an optional permission update list can be established.

Trust is always associated with risk. Therefore trust based systems just offer soft-security mechanisms and are appropriate to secure objects that have a small value. The delegation system is not designed to substitute but to complement traditional access control mechanisms.

Future work will focus on introducing more permission constraints like a stronger context awareness or situation specific permissions. The implementation will be extended to support more services and platforms and will be integrated in our smart office environment using a service management middleware.

5. References

[1] E. Barka, R. Sandhu, "Role-Based Delegation Model/ Hierarchical Roles (RBDM1)", in Proceedings of 20th Annual Computer Security Applications Conference, Tucson, AZ, USA, 2004.

[2] M. Blaze, J. Feigenbaum, J. Ioannidis, A. D. Keromytis, "The Role of Trust Management in Distributed Systems Security", Secure Internet Programming, 1999.

[3] D. Chaum, “Security Without Identification: Transaction Systems to Make Big Brother Obsolete”, Communications of the ACM, vol. 28 no. 10, 1985.

[4] K. Fujimura, H. Kuno, M. Terada, K. Matsuyama, Y. Mizuno, J. Sekine, "Digital-Ticket-Controlled Digital Ticket Circulation", in Proceedings of 8th USENIX Security Symposium, Washington D.C., 1999.

[5] A. Jøsang, R. Ismail, C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision”, to appear in Decision Support Systems, 2005.

[6] L. Kagal, S. Cost, T. Finin, Y. Peng, "A Framework for Distributed Trust Management", in Proceedings of IJCAI-01, Workshop on Autonomy, Delegation and Control, Montreal, Canada, 2001.

[7] S. Lo Presti, M. Cusack, C. Booth, "Trust Issues in Pervasive Environments", Deliverable WP02-01, Trusted Software Agents and Services for Pervasive Information Environments Project, University of Southampton, 2003.