Security and privacy rights management for mobile and ubiquitous computing

Michael Fahrmair, Wassiou Sitou, and Bernd Spanfelner

Technische Universität München, Department of Informatics,
Boltzmannstr.3, D-85748 Garching (Munich), Germany
{fahrmair|sitou|spanfeln}@in.tum.de

Abstract. A new computing era after mainframes, PC's and mobiles is becoming more and more anticipated since the beginning of the 21st century: Ubiquitous Computing. A common characteristic behind this approach is that, it is based on a substantially more flexible system understanding, whereby the thought of the system as a tool moves into the background and the needs and wishes of the user step into the foreground. In this paper we describe a generic mechanism for security and privacy rights management in mobile and ubiquitous computing environments that is based on the idea of seeing context information as intellectual property and enforcing privacy- and ownership of users. This is achieved by a security and context management architecture that enables each described object in a context to directly or indirectly control the process of creating a package of sensible or personal information and licensing it (via existing DRM concepts) to any service provider that is interested in consuming this information.

Keywords: ubiquitous, pervasive, ambient, context-aware, adaptation, reconfiguration, security, privacy, DRM, adaptive systems

1 Introduction

Adaptation in a common sense is defined as an act of changing (structure, form, or habits) to fit different environmental conditions [7]. For technical systems in general such environmental conditions are usually referred to as *context* (see also [3] and [6]).

The idea of adaptive and ubiquitous systems is already a subject of intense research for several years. Recently, some works on how adaptation can be enhanced were published [4] and rise the question on how information that is distributed all over a ubiquitous system can be protected especially regarding the user's privacy.

In this paper we therefore first examine a short scenario to work out the exact requirements of PRM (Privacy Rights Management). Based on these requirements, we present an architecture to enable users to express and to enforce conditions and constraints for the use of their data. Afterwards some considerations about security aspects are made and in the concluding part, a first evaluation of the system is given.

2 Scenario and Requirements

The scenario contains a single user located in a public place like the center of a city. There some location based services which rerquire the user to submit specific information are offered. These services may be anything like buying a ticket for museum entrance online or just simply map navigation. Usually the user has no idea what exactly is done with his data. A service may store or process the provided data in some way that is not intended by the user. As well a service may pretend to be another one that is commonly trustworth and thus exploiting lesser privacy concerns (e.g. run by a trustwoth company or the city administration). Furthermore there may be services that demand information but act automatically rather than waiting for a user's request. From this scenario the following requirements can be identified:

- **Protection against misuse:** There should be a possibility for a user to express conditions and constraints for the usage of context data. This includes proper identification of services.
- **Identification of pirated datasets:** If a service was able to circumvent the protection there should be a possibility to identify that service. (Not covered in this paper, for details see [5]).
- **Adjustment of laws:** Under certain circumstances this will provide additional security. (Not covered in this paper, for further in formation see [5]).
- **Ease of use:** A protection system with maximum security but high complexity of handling is of no use.

3 A Privacy Rights Management (PRM) System for Ubiquitous Computing

In this section an architecture is described in short that is able to protect user data from misuse and to express and enforce conditions and constraints for valid uses or deny data if no adequate level of trust can be recognized. The basic idea is to adapt a generic Digital Rights Management (DRM) system for the use in a ubiquitous environment. The private context data is therefore treated as some kind of digital property. This section describes the components involved in the system and their cooperation. This approach has already been worked on in a similar way e.g. by [9] and [10] but both took a more optimistic point of view where market dynamics and laws would enforce the rights and constraints rather than a technical solution.

In ubiquitous computing a user needs some device that allows the system to interact with the user. This device can be anything from a device that only allows identification or positioning of the user like active bats [2] to a fully featured hand held or other mobile device that is capable of intense interaction with the user. We have to distinguish these two classes of user devices. One enables active requests of services and the other does not. In the first case the user can decide to use a service actively and this results in the generation of a signed ticket consisting of a unique number and a time stamp. This ticked is sent to the service. In the second case no active choice of the user is possible or intended by the service. Here the service starts acting automatically. Furthermore if possible, authentication between user device and service must be done. If this is not possible due to lacking computation power or interaction facilities of the device this will be delegated, but this will result in a loss of security.

Once a service gets active either by being sent a ticket or automatically, this service has to contact a license server that is run (under control of) by the user. Authentication between both is mandatory for ensuring the service to be the one it pretends to be. If available the service has to hand over the ticket to the license server. If the ticket was not handed over (user did not actively request the service) the license server can ask a special user service that stores information about services that a user is willing to use without explicit request. If the service is not designated for use, no further steps are taken by the license server and therefore the service will not receive any data. If it is designated, a license is generated that describes the conditions and constraints for data usage in a Rights Expression Language (REL) [1]. Furthermore a key for a symmetric encryption is generated and enclosed in the license. The license server stores meta data like the name of the service, service description, generated key etc. in a special package and sends this to a context server. An index to this meta data is generated, signed and sent together with the license to the service.

Now the service can send the recieved index to the context server which holds the required data. If there is more than one context server involved, the meta data was sent to all of them and hence the index now must be sent to all of them as well. The signed index is a prove for the context server(s) that the service was checked and it points to the meta data that is needed to collect the desired data. For this purpose the service description is utilized. The data is assembled in a container that is encrypted with the key from the meta data. This container is now sent to the service. The service can now utilize the key from the license to get access to the data.

4 Security issues

One now can state that the system does not provide any advances over a normal access control system since nothing would keep the service from using the key to extract the data and store it elsewhere, distribute it to unlicensed third parties or misuse it in some other way. This assumption would be correct if there wasn't a further not yet mentioned fact to prevent this.

In DRM-systems a content provider has to trust rendering hard or software to properly manage the content and the license. This is also true for the PRM-system. In DRM-systems the trust is enabled through the system developer either by developing the hard- or software itself or by certifying third party rendering hard- and software. This is not possible in PRM since everybody should be able to develop services. Therefore a trusted third party is needed.

It acts like a Certification Authority (CA) and tests the services for back doors or improper functionality. Then a certificate is issued that contains information about the level of trust of the service and in some cases a hash value of the software.

Now the license server comes back into the game. For authentication purposes a certificate is needed anyway and here the extended certificates are used. A user has to deploy a policy which rates the privacy of any of the user's data. Of course, some intelligent software like an assistant is needed to guide a user through an initial assessment process and to enable proper rating even for unexperienced users. According to this rating and the level of trust the certificate claims, the license server can either grant or deny a license.

Obviously there must be a possibility to check the service during runtime to ensure that the service software has not been manipulated after certification time. This can be done by comparing the hash value from the certificate with a hash value calculated e.g. by a function of the OS the service is running on or some trusted hardware. The levels of trust that are stated by the CA then are in detail: Level 1: software not checked, only authentication possible. Level 2: software checked but no on-line hash verification possible. Level 3: software checked and secure hash verification online possible.

According to the levels a license server may only distribute public data to a service of level 1 and on the other hand very private data only to services of level 3. This method ensures that very private data is only provided to high security services where proper usage of data and license is guaranteed. Services that normally do not need confidential data do not need to be reviewed by the CA and hence the certification complexity for them is not as high as for services that want to deal with confidential data.

To be able to apply this system to a wide range of devices and situations we also introduced class marks which consider different hardware and networking situations (see [5]). However this is out of the scope of this document.

5 conclusion

We described a system that enables description and enforcement of conditions and constraints for the use of confidential and private context data. The fact that for full trustability a service has to be reviewed and certified by a CA is often not affordable for small services. But this is often not necessary e.g. for service in a trusted environment (home, friends). Services that only process less confidential data only need a certificate that ensures their identity. Only services that process highly confidential data must face the full certification process. The user has the choice via the licence server to provide data or not. The enforcement of trust relies on the CA and the online check of hash values but does not necessarily require trusted hardware. Therefore the system fits for a wide spread spectrum of services without changes and thus considers the premise of ubiquitous computing that services should be available to anybody at any time in any situation.

References

1. Guth, S.: Rights Expression Languages. In: Becker, E. (Ed.); Buhse, W. (Ed.); Guennewig, D. (Ed.); Rump, N. (Ed.): Digital Rights Management: Technical, Economica, Legal and Political Aspects (LNCS2770), Springer, 2003. ISBN 3-540-40465-1, P. 101-112
2. AT&T Labs.: The Bat Ultrasonic Location System. Web Resource, http://www.uk.research.att.com/bat/
3. Dey, A.: Providing Architectural Support for Building Context-Aware Applications. PhD thesis, College of Computing, Georgia Institute of Technology, December 2000.
4. Fahrmair, M.: Kalibrierbare Kontextadaption fuer Ubiquitous Computing. Dissertation, Faculty of Informatics, Technische Universitaet Muenchen, Jan 2005.
5. Spanfelner, B.: Digitales Rechtemanagement fuer Mobile- and Ubiquitous Comuting. Diploma Thesis, Faculty of Informatics, Technische Universitaet Muenchen, Feb 2005.
6. Lieberman, H., Selker, T.: Out of Context: Computer Systems that adapt to, and learn from, Context. IBM Systems Journal, 39(3-4): 617-632, 2000.
7. Merriam-Webster: Collegiate Dictionary - Eleventh Edition. Merriam-Webster, Inc., 2003.
8. G. Karjoth, M. Schunter, and M. Waidner. Privacy-enabled services for enterprises. In International Workshop on Trust and Privacy in Digital Business (Trustbus 2002), pages 483-487, IEEE Computer Society, 2002.
9. Jason I-An Hong. An Architecture for Privacy-Sensitive Ubiquitous Computing. Dissertation (Spring 2005), http://www-2.cs.cmu.edu/ jasonh/publications/jihdiss.pdf.
10. M. Langheinrich. A Privacy Awareness System for Ubiquitous Computing Environments. In G. Borriello, L. E. Holmquist, editors, Proceedings of UbiComp 2002, pages 237-245 or http://citeseer.ist.psu.edu/langheinrich02privacy.html