ERCIM "Alain Benoussan" Fellowship Scientific Report

Fellow: Ludwig Seitz
Visited Location: SICS, Kista, Sweden
Duration of Visit: 1. November 2005 - 30 April 2007

1 Scientific activity

In the course of my fellowship at SICS I have been working in the Security, Policies and Trust laboratory (SPOT). There the main focus of my work has been the XACML access control standard. SICS has joined the standardisation committee and is currently driving the developement of version 3.0 of the standard. This version will add delegation mechanisms to XACML. In order to support this activity I have implemented the current version of the standard draft, based on Sun Microsystems Java implementation of XACML 2.0. This product called *SICSACML* is available under open-source licence from the SICS webpage[1]. Until today it has been downloaded over 100 times since July 2006. Another open-source product that I have developed during my stay at SICS is the AssertionServer, a tool for providing and managing attribute assertions for access control[2]. This tool has been downloaded over 80 times since July 2006.

I have participated in a SICS project funded by the Swedish Defence Materiel Administration, where I have delivered a report on *Security threats to access control systems* and a report on *Access control for limited devices*.

Furthermore I have been one of the main contributors from SICS side to the PRIMA-Net project, funded by the Swedish Governmental Agency for Innovation Systems (Vinnova)[3]. This project deals with access control for mobile network management. Within the project I have delivered a report on *Access control architectures for mobile network management* which is available from the project website. I am currently finishing a report on *Providing XACML access control for the NETCONF protocol*, which will be available from the project website soon.

I am the co-author of the successful Vinnova project proposal TrustDis [4]. However due to the workload of other projects I have not been contributing to the project until now.

The last project I am actively participating in is funded by SICS internally. It deals with applications of access control for physical security. In the course of this project we produced a patent that is currently submitted to the Swedish patent office and awaiting approval.

Furthermore I have been scientific supervisor for two master students, Bertrand Leneveu who has been working on *Integration of the XACML-based Policy Decision Point, Delegent, with LDAP* and Adriaan Slabbert who is currently working on *Distributed Physical Access Control: A Constrained Resource Solution*.

2 Publication(s) during your fellowship

- Published as Springer LNCS, proceedings of FAST2006 workshop

  A Classification of Delegation Schemes for Attribute Authority

  Ludwig Seitz, Erik Rissanen, Babak Sadighi.

  Abstract:

[1] http://www.sics.se/spot/xacml_3_0.html
[2] http://www.sics.se/spot/assertion_server.html
[3] http://www.sics.se/primanet
[4] http://www.sics.se/trustdis/

Recently assertions have been explored as a generalisation of certificates within access control. Assertions are used to link arbitrary attributes (e.g. roles, security clearances) to arbitrary entities (e.g. users, resources). These attributes can then be used as identifiers in access control policies to refer to groups of users or resources.

In many applications attribute management does not happen within the access control system. External entities manage attribute assignments and issue assertions that are then used in the access control system. Some approaches also allow for the delegation of attribute authority, in order to spread the administrative workload. In such systems the consumers of attribute assertions issued by a delegated authority need a delegation verification scheme.

In this article we propose a classification for schemes that allow to verify delegated authority, with a focus on attribute assertion. Using our classification, one can deduce some advantages and drawbacks of different approaches to delegated attribute assertion.

- Patent submission P06-094 to the Swedish patent office, patent registration process not yet completed.

  Access control system and method for operating said system.

  Babak Sadighi, Cao Ling, Ludwig Seitz.

  Abstract (subject to changes):

  This patent discloses an invention that allows door access control using mobile phones. The administrator uses the mobile network to transfer personalised access permissions to the mobile phone, which in turn communicates with the door-lock through NFC short-range technology. The advantages of this invention are that the distribution of access rights does not require the recipient and the administrator to meet in person, as with other systems like keys, access cards, etc. Furthermore since the door and the phone use the NFC technology to communicate, neither the door nor the phone need network connection at the time of access.

3 Attended Seminars, Workshops, and Conferences

- *First International Workshop on IT-solutions for Physical Security* March 2006, Stockholm. http://www.sics.se/phys-sec/2006/
- *Workshop on RFID Security 2006*, 12-14. July 2006 Graz, Austria. http://events.iaik.tugraz.at/RFIDSec06/
- *CERICS workshop*, Royal Holloway, University of London, 20-21 July 2006. http://www.isg.rhul.ac.uk/node/151
- *FAST2006 workshop*, August 26-27 2006, Hamilton, Ontario, Canada. http://www.iit.cnr.it/FAST2006/