

An Authorization Model for Lightweight Tasks in a Face-to-face Collaborative Wireless Environment

Stacey Scott
EDGE Lab, Simon Fraser University

CMPT 470/882 Class Presentation
March 23, 2001



Outline

- Motivations
- Security issues in wireless networks
- Traditional authorization models
- Authorization models for collaborative systems
- An authorization model for face-to-face wireless collaboration
- Basic implementation details (plans)



"Personal" Devices Facilitate "Group" Activities

- Traditional computers provide little support for face-to-face collaboration
- Mobile devices are becoming ubiquitous
- Most research on mobile devices focuses on the "personal" aspect (e.g.: PDAs as organizers)
- As the connectivity of these devices increases, they offer potential to facilitate collaboration
- Bluetooth wireless standard to provide infrastructure to support face-to-face group activities such as ad-hoc networking



Potential Scenario



Some Requirements for this Scenario

- An easy way to detect a machine's Internet address
 - ActiveTags
- A flexible security model
 - Allow access to known, "trusted" collaborators
 - Flexible enough to allow, perhaps limited or temporary, access to "visiting" or "untrusted" collaborators



Wireless LAN Security Threats (Vainio '00)

- Disclosure threats
 - eavesdropping
- Integrity threats
 - information is intercepted and altered by a (malicious) third party before reaching intended destination
- Denial of Service threats
 - battery attacks



Authentication vs. Authorization (Sikkel '97)

- **Authentication**
 - You are who you say you are
 - Masquerading
- **Authorization**
 - You are allowed (*have access rights*) to:
 - the operation you are trying to perform
 - the data that you are trying to access

Traditional Authorization Models

- **User-based Authorization**
 - Permissions to system resources (files, processes) are based on system users
 - Lampson access control matrix (Lampson '74)

	File 1	File 2	File 3
Sandy	owner, read, write	read	execute
Mary	read	read	execute
Blair	read, write	write	

capabilities →

↑
access control list (ACL)

Traditional Authorization Models (Cont'd)

- **Role-based Access Control (RBAC)** (Sandhu et al '96)
 - simplifies the management of permissions
 - separates the system users from system resource permissions
 - allows users to be easily assigned appropriate roles
 - permissions of roles tend to be more stable than that of individual users
 - can be ACL-based or capabilities-based

Access Issues in Collaborative Apps

- Higher access control demands than traditional systems because of the chaotic environment
- Users often change roles during the course of the session -- requires flexible permissions
- Access of system objects often depends on actions of other users -- requires dynamic access control definitions

Authorization Models for Collaboration

- **Access control model for synchronous collaborative applications** (Shen & Dewan '92)
 - one of first access control models developed for a groupware application
 - complex model that extended Lampson's access control matrix to provide a model which offered fined-grained control of system objects
 - introduced collaboration rights
 - used positive and negative rights

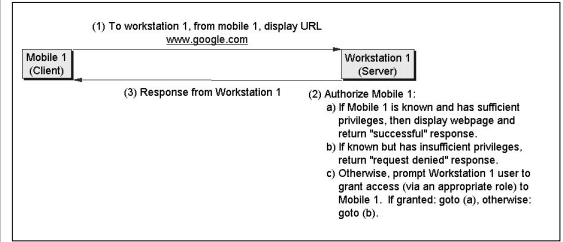
Authorization Models for Collaboration

- Subsequent research has introduced the following ideas to control the complexity of access control in collaborative systems
 - policies for static and dynamic roles (Edwards '96)
 - negative access rights and delegation (Sikkel '97)
 - RBAC in a team-based organization (Wang '99)
 - spatial metaphors (Bullock & Benford '99)
 - automated verification of policies (Godefroid et al '00)
- Many of these models were developed for control of complex, distributed groupware environments

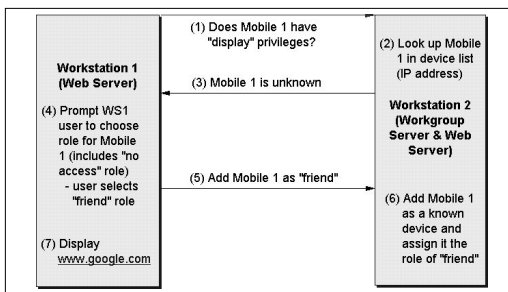
Leveraging the “Real-World” Aspects of F2F Collaboration

- No need for digital authentication (e.g., digital certificates) since authentication can be done in person
- Some implicit “trust” if you’ve allowed the Client user into your office/lab/home, etc.

Authorization Model for F2F Collaboration (Basic Concept)



Authorization at the Server



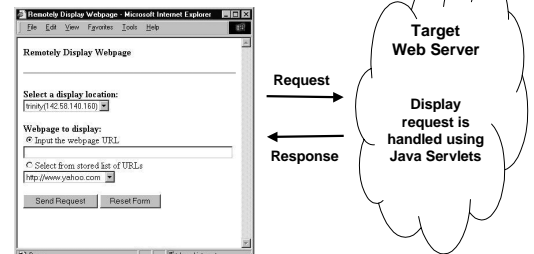
Resolution of Access Control

- **Course-grained access control (centralized)**
 - One access control list is kept by an access control server
 - Grants access to all resources served by the central access control server
- **Fine-grained access control (de-centralized)**
 - Access control lists are kept at each server in the work group.
 - Could still use a centralized list of *static* users/devices, but each server could also grant “local only” access to clients

Implementation (in progress)

- Since tasks are “lightweight” we can exploit the ubiquity and security provided by the Web (protected system files and programs)
- Client/Server model that assumes all “target” devices (such as WS1 in the example) are running their own Web servers
- System Hardware:
 - IEEE 802.11 short-range (150-300 feet) wireless network
 - Compaq iPaq (Windows CE handheld device) and Toshiba Pentium laptop with Intel wireless network cards

Implementation (Cont'd)



Acknowledgements

- Wing Lee, for the great Orion setup page!
- Arman Danesh, Colin Swindells, Felix Lau for great discussions and research material
- Daryn Mitchell for the Scenario drawing

References

- Barkley, J.F., et al (1997). Role Based Access Control for the World Wide Web. *Proc of NIST/NSA 1997*.
- Bullock, A. and Benford, S. (1999). An access control framework for multi-user collaborative environments. *Proc of Group 1999*, pp. 140-149.
- Edwards, W.K. (1996). Policies and Roles in Collaborative Applications. *Proc. of CSCW 1996*, pp. 11-20.
- Goddroid, P., et al (2000). Ensuring Privacy in Presence Awareness Systems: An Automated Verification Approach. *Proc of CSCW 2000*, pp. 59-68.
- Lampson, B.W. (1974). Protection. *ACM Operating Systems Review*, Vol 8, No. 1, pp. 18-24.
- Shen, H. and Dewan, P. (1992). Access Control for Collaborative Environments. *Proc of CSCW 1992*, pp. 51-58.
- Sikkil, K. (1997). A Group-based Authorization Model for Cooperative Systems. *Proc of ECSCW 1997*, pp. 345-360.
- Sandhu, R.S., et al (1996). Role-Based Access Control Models. *IEEE Computer*, Vol 19, No. 2, pp. 38-47.
- Vainio, J.T. (2000). Bluetooth Security. Retrieved March 21, 2000 from <http://www.niksula.cs.hut.fi/jtv/bluesec.html>
- Wang, W. (1999). Team-and-Role-Based Organizational Context and Access Control for Cooperative Hypermedia Environments. *Proc. of Hypertext 1999*.

Thank You!