CS590U

Access Control: Theory and Practice

Lecture 5 (Jan 25)

Bell-LaPadula

Projects

- Ji-Won Byun
    - Enterprise Authorization Management
- Jiangtao Li
    - Trust negotiation
- Abhilasha Bhargav Spantzel
    - Extension of X-TNL language for Negotiation in a Federation
- Qihua Wang
    - Insider Threat Assessment

Projects

- Ian Molloy
  - Smart card
  - Privacy and access control in CORBA
  - RMI & EJB
- Ryan Riley
  - Smart card
  - LDAP Server

Projects

- Paul Kuliniewicz
  - High-level language for specifying SELinux policies
  - RMI & EJB
  - Privacy-Centric Access Control
- Yu Zhang
  - Data stream systems
  - Privacy-Centric Access Control
  - RMI & EJB
- Jing Dong
  - Workflow & CSCW systems
  - Smart cards
  - RMI & EJB

Assignment I Review

Terminologies

- Identification:
  - ascribing an ID to a human being or to another computer or network component
- Authentication:
  - binding an ID to an active entity in the system
- Access control:
  - determining whether an active entity can access resources
  - effective access control requires effective authentication

Frustrations with Access Control

- UNIX: difficult for share files with specific users
- Windows
  - Windows 2000: cannot install USB flash disk as an ordinary user, because this is adding a new device to the system
  - cannot allow install software without local admin authority
  - unpredictable behavior about sharing, refusing access for no reason

Frustrations with Access Control

- Unable to access ACM/IEEE from off-campus networks
- Ineffective wireless access control based on MAC
- No knowing how personal information is stored and used
  - information is stored in too many places
- CGI: CGI program not allowed to create/modify files on the server

Vulnerabilities

- set-uid processes
  - choosing between coarse granularity and complex policies
- Lack of access control for JPEG engine and MS Office applications
  - need to know what an application is supposed to do
- With application wrappers in Windows
  - IIS loads many DLL’s in the address space of another process, the DLL Host, (using remoting), which makes achieving least privilege difficult

About Groups, Privileges, Abilities, Roles

- They are all indirections adding between subjects and permissions
  - middle layers are again structured

- Some times, different restrictions are assigned to different names
  - e.g., one can choose to activate a role or not, but one cannot deactivate a group

Things to be covered later

- Role Based Access Control
- Access Control in Windows

Problem from Gollmann Book

- Consider
  - A grant read w/ grant to B
  - B grants read w/grant to C
  - C grants read to D
  - A revokes read-grant from B

Go to the Bell-LaPadula Note

End of Lecture 5

- Next lecture:
  - Harrison-Ruzzo-Ullman