CS590U

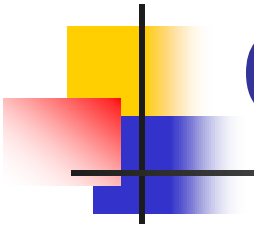
Access Control: Theory and Practice

Lecture 1 (Jan 10)

Introduction to the Course

Instructor Info

- Ninghui Li
  - Email: ninghui@cs.purdue.edu
  - Office phone: 765-496-6756
  - Office: REC 217C
- Office hour
  - Tuesday 4:20pm to 4:50pm
  - Thursday 4:20pm to 4:50pm
  - By appointment

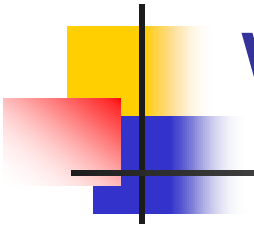


Coursework

- Readings
  - before each lecture
- Assignments (30%)
  - problems
  - review of assigned papers
- Mid-term exam (30%)
- A project (40%)

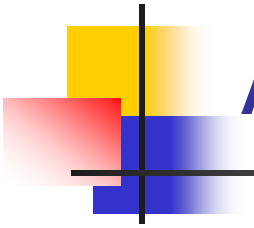
Check the course homepage

Why a Course on Access Control?



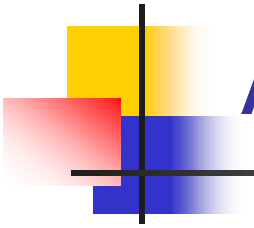
What is Access Control?

- Quote from Security Engineering by Ross Anderson
  - Its function is to control which principals (persons, processes, machines, ...) have access to which resources in the system --- which files they can read, which programs they can execute, and how they share data with other principals, and so on.



Access Control is Pervasive

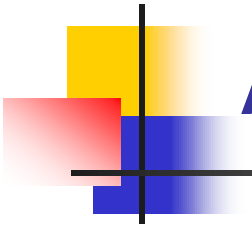
- Application
  - business applications
- Middleware
  - DBMS
- Operating System
  - controlling access to files, ports
- Hardware
  - memory protection, privilege levels



Access Control is Important

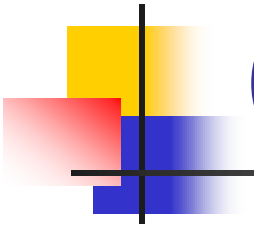
- Quote from Security Engineering
  - Access control is the traditional center of gravity of computer security. It is where security engineering meets computer science.
- TCSEC evaluates security of computer systems based on access control features + assurance

Access Control is Interesting

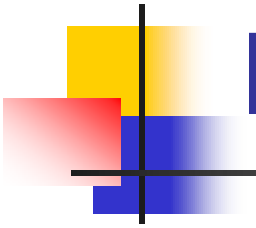


- Has (relatively) well-developed theories
  - 30+ years history
  - some (quite involved) theory (apparently) not useful for other fields
- Many interesting and deep results
- Many misconceptions and debates
- A large percentage of published works contain serious errors
  - Corollary: Be skeptical, don't believe too much what others have said, try form your own opinions

Principles of Access Control (Saltzer and Schroeder 75)



1. Economy of mechanism
   - keep the design as simple and small as possible
2. Fail-safe defaults
   - default is no-access

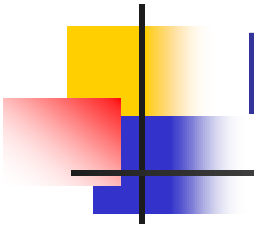


Principles of Access Control

3. Complete mediation
   - every access must be checked
4. Open design
   - security does not depend on the secrecy of mechanism

Principles of Access Control

5. Separation of privilege
   - a system that requires two keys is more robust than one that requires one
6. Least privilege
   - every program and every user should operate using the least privilege necessary to complete the job

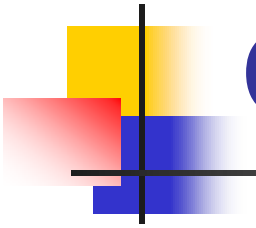


Principles of Access Control

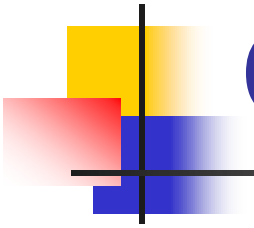
7. Least common mechanism
   - "minimize the amount of mechanism common to more than one user and depended on by all users"
8. Psychological acceptability
   - "human interface should be designed for ease of use"
   - the user's mental image of his protection goals should match the mechanism

An Incomplete History of Access Control Research

Earlier Years: Time-Sharing Operating Systems

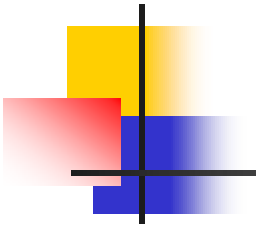


- Reference monitors (1972)
- Access matrix (1971)
- Discretionary access control
  - trojan horse can leak information



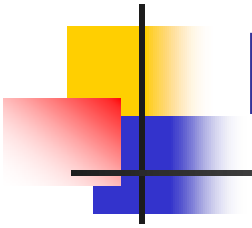
Confidentiality

- Bell-LaPadula Model
- Noninterference (1982)
- Nondeducibility (1986)
- Covert channel
- Proving information flow properties of systems and programs



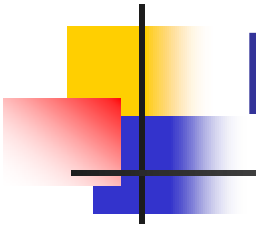
Integrity

- Biba model
- Clark-Wilson
- Chinese Wall



Database Access Control

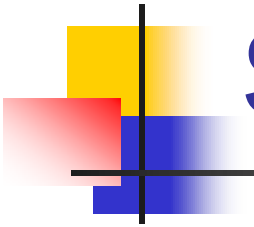
- System R approach: grant/revoke, view
- Ingres approach (query rewriting)
- Multilevel databases
- Object/relational databases
- Real systems
  - SQL grant/revoke, view, stored procedures, fine-grained access control
- Privacy centric



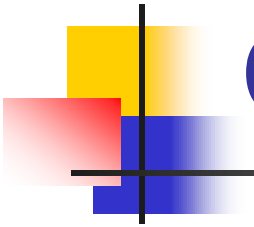
Role-Based Access Control

- First in database context
- Then a generic access control approach
- Constraints
- Administration
- Extensions

Access Control in Distributed Systems

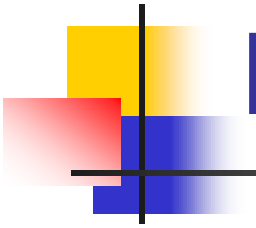


- ABLP Logic
- Trust management
  - PolicyMaker, KeyNote, QCM/SD3, Delegation Logic, Binder, RT
- Automated trust negotiation



Other Topics

- Workflow systems
- Firewall
- Cryptographic approach



End of Lecture 1

- Next lecture:
  - Access matrix
  - Partial order and lattices
  - State transition systems