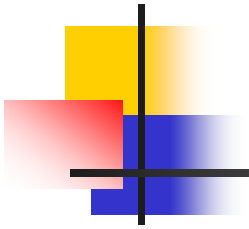
CS590U

Access Control: Theory and Practice

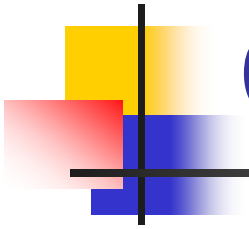
Lecture 1 (Jan 11)

Introduction to the Course



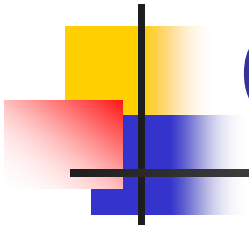
Instructor Info

- Ninghui Li
  - Email: ninghui@cs.purdue.edu
  - Office phone: 765-496-6756
  - Office: REC 217C
- Office hour
  - Tuesday 4:20pm to 5:20pm
  - Thursday 4:20pm to 5:20pm



Coursework

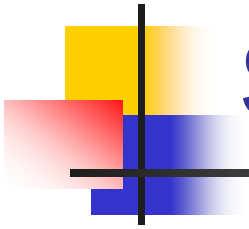
- Lectures & participations (10%)
- Readings
  - before each lecture
- Eight assignments (40%)
  - problems
  - review of assigned papers



Coursework

- A course project (individual)
  - Pre-proposal — Jan 20
  - Proposal — Feb 8 — 10%
  - Presentation — Apr 19 to 28 — 10%
  - Final report — Apr 30 (Sat) — 30%

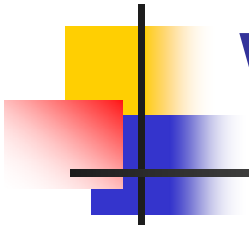
Pre-proposal (Due Jan 20) Submit paper copy before class



- List 1 to 3 project topics you find interesting
  - Why these topics interest you?
  - What are your plans?
  - What related backgrounds do you have?
- Propose new project ideas
  - Background, problem, plan, references ...

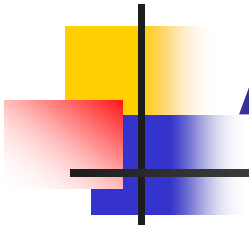
Check the course homepage

Why a Course on Access Control?



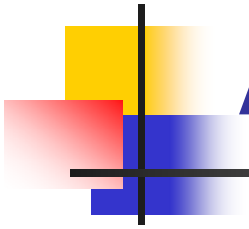
What is Access Control?

- 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.



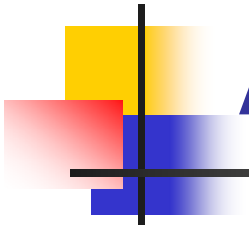
Access Control is Pervasive

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



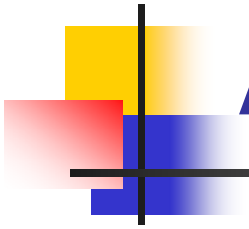
Access Control is Important

- 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

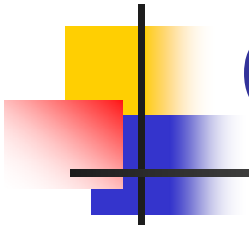


Access Matrix

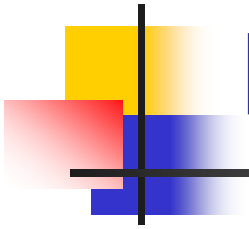
- A set of subjects S
- A set of objects O
- A set of rights R
- An access control matrix
  - one row for each subject
  - one column for each subject/object
  - elements are right of subject on another subject or object

An Incomplete History of Access Control Research

Earlier Years: Time-Sharing Operating Systems

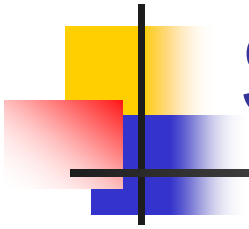


- Reference monitors (1972)
- Access matrix (1971)
- Discretionary access control
  - trojan horse can leak information
- Access control list
- Capabilities
- Multics



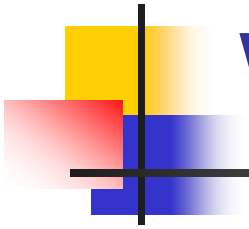
Military Wants Confidentiality

- Mandatory access control
- Label-based access control
- Bell-LaPadula (1973+)
- Covert channel
- Verifying security
- Security kernels
- TCSEC (1983)



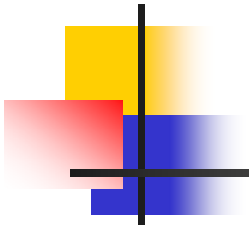
Safety Properties

- The HRU undecidability result (1976)
- The Take-Grant scheme (1977)
- Grammatical systems
- Schematic Protection Model (1985)
- Typed Access Matrix (1992)
- Security Analysis
  - in Trust Management
  - in Role-Based Access Control
  - in Discretionary Access Control



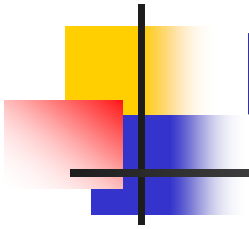
What About Integrity?

- Biba integrity model
- High watermark/low watermark
- Clark-Wilson
- Chinese Wall
- Domain-Type enforcement



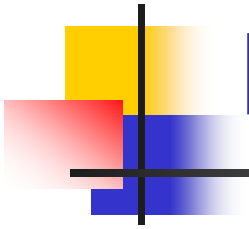
Information Flow Problems

- Noninterference (1982)
- Nondeducibility (1986)
- Composing security
- Information flow in programs
  - Denning's work
  - Language-based security



Database Access Control

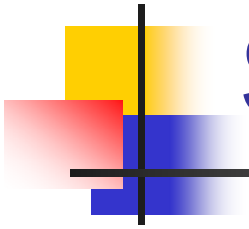
- System R approach: grant/revoke, view
- Ingres approach (query rewriting)
- Multilevel databases
- Object/relational databases
- Real systems
  - SQL grant/revoke, view, stored procedures, fine-grained access control
- Privacy centric



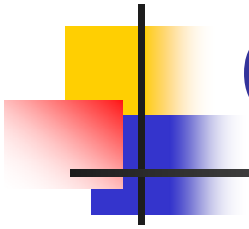
Role-Based Access Control

- In database context [1990]
- Generic access control approach [1992]
- Constraints
- Administration
- Relationships with DAC and MACs
- Extensions

Access Control in Distributed Systems



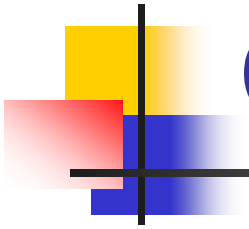
- ABLP Logic
- Trust management
  - PolicyMaker, KeyNote, QCM/SD3, Delegation Logic, Binder, RT
- Automated trust negotiation



Other Topics

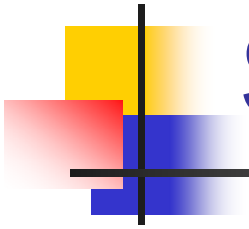
- Java
- Operating system wrappers
- XML access control
- Workflow systems
- Computer Supported Collaborative Work
- Firewall
- Cryptographic approach

Why is Access Control Complex?



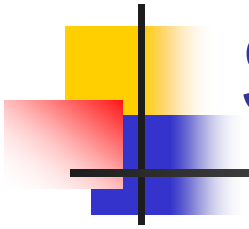
Objects are often complex

- Objects may be structured:
  - directories/files
  - database, table, row, column, view
  - XML documents
- Identifying objects may be hard



Subjects are complex

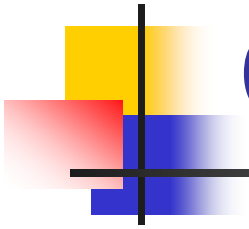
- What are subjects?
  - human users
  - principals (e.g., accounts, public keys)
  - processes
- What are the relationships among subjects?
  - whose authority to use?
- On what basis does one grant access?



Systems may be large

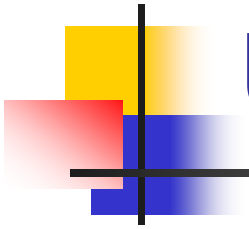
- Number of subjects may be hundreds of thousands

Access Control States May Change



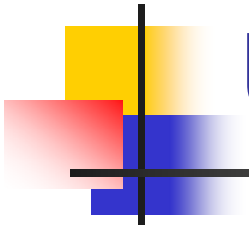
- Who can make changes?
- What kinds of changes can be made?
- Often not clearly specified
  - lead to many many misconceptions in access control

Security Objectives Often Unclear

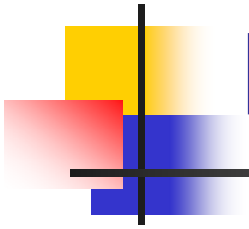


- What properties do we want an access control system to have?
  - allow legitimate sharing, forbid illegitimate sharing
  - what sharings are legitimate?
- The criteria of goodness is often unclear.

Very Limited Understanding of Usability Issues



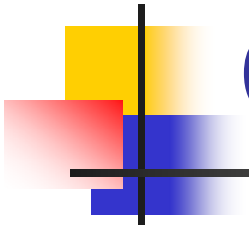
- Not much thought has been put into usability issues.
- Not clear what can/should be done.



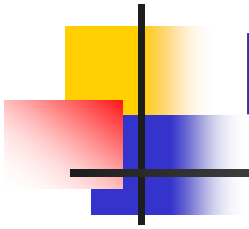
MisConceptions that

- MisConceptions that we are fighting
  - Safety analysis is hard
  - RBAC is more expressive than DAC
- Debates
  - Bell-LaPadula vs. System Z
  - Capability vs. ACL

Grand Challenges in Access Control



- Operating system access control
  - Unix is bad, Windows seems worse, SELinux is unusable, is there any hope?
- Enterprise security management
  - RBAC is useful but limited, what is the next RBAC?
- A uniform approach to database access control
- A unified theory/methodology that can be fruitfully applied most of the times
- Meaningful verification techniques
- Usability theory/facts/guidelines



End of Lecture 1

- Next lecture:
  - my funded research projects
  - project topics