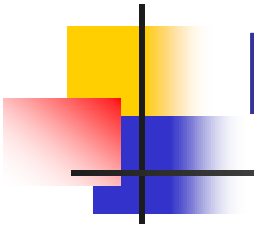
CS590U

Access Control: Theory and Practice

Lecture 26 (April 14)

Review of the Course

Fine-Grained Access Control in Databases



- Oracle VPD
  - (PL/SQL) programs as policies
- Ingres
  - authorization views are used to rewrite queries
- Hippocratic databases
  - privacy policies determine which fields can be seen and which cannot
- Non-Truman
  - views determine which queries can be answered and which cannot

Problems and Issues with Existing Approaches

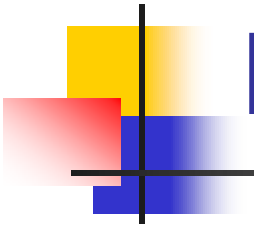
- Fail to answer a query when “it can be answered”
- Return results that seem to be wrong
- Aggregates in queries cause trouble
- May need to return partial information

Query Modification- Aggregates

- **Four possibilities**
  1. Allow aggregates without restriction
  2. Allow aggregates without restriction if the minimum number of values aggregated exceeds some threshold
  3. Allow aggregates without restriction if they are unqualified (e.g. are aggregates over a whole relation)
  4. Allow aggregates only with access control qualifications appended inside the function

Open Problems in Fine-Grained Access Control in DB

- What are the intended meanings of a policy?
- I.e., given a policy, a DB state, and a query, what should be the correct answer?
  - return correct information
  - only reveal information that is allowed to be revealed
  - return maximum amount of information
- It is difficult to formalize the above properties and achieve them



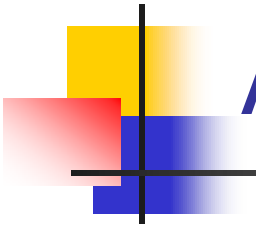
Firewalls

- Firewalls do access control at packet level
- Typical firewall policies are specified using a ordered ruleset
  - understanding a rule is difficult, as it interacts with other rules before it
- Similar techniques are used in many places, e.g., ordered ACL in IBM Tivoli, MS Windows
- Decision Diagrams Provide an alternative to ordered rulesets

Review of The Course

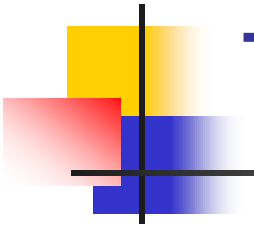
Access control exist in many settings

- Operating systems
  - dynamic: processes
  - static: users sharing resources
- Database systems
- Mobile code
- Distributed systems
- Enterprise information systems
- Almost any information systems



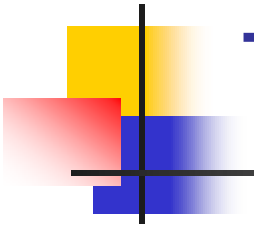
Access Control

- Theory of access control consists of scattered, often loosely connected, and occasionally useful pieces
  - just like the information security field in general
- Access control in real-world systems use some basic ideas from theory, and can be complicated and inelegant



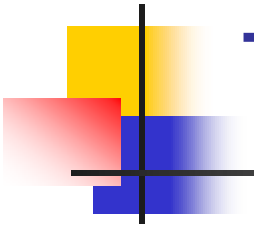
Topics We Have Covered

- Access matrices
- Access control schemes
- The Graham-Denning DAC schemes
- The Bell-LaPadula MAC model
- Safety analysis in HRU, DAC, Take-Grant
- Noninterference and nondeducibility
- Confinement and covert channels
- Biba integrity, Clark-Wilson, Chinese Wall



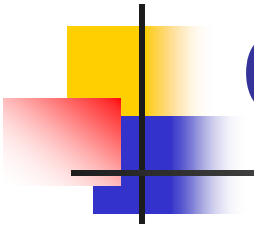
Topics We Have Covered

- Role-Based Access Control
  - Models
  - Separation of Duty & Constraints
  - Administration of RBAC
- Trust Management
  - PolicyMaker, SDSI, its semantics, SPKI
  - RT0, distributed discovery, the RT languages
  - Security analysis
  - Automated Trust Negotiation



Topics We Have Covered

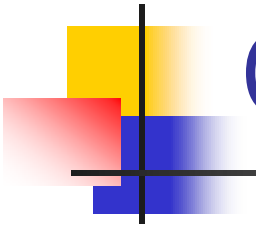
- Expressive power
- Capability-based operating systems
- DB Access Control:
  - Griffiths-Wade scheme
  - Oracle
  - Query rewriting



Other Topics

- Mobile code, e.g., Java
- Operating system wrappers
- XML access control
- Workflow systems
- Computer Supported Collaborative Work
- Cryptographic approach
- Grid computing

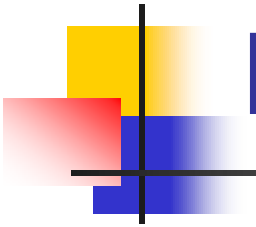
Grand Challenges in Access Control



- Operating system access control
- Enterprise security management
- Database access control
- A unified theory/methodology that can be fruitfully applied most of the times
- Meaningful verification techniques
- Usability theory/facts/guidelines

Projects That are Ongoing/Being Contemplated

- Fine-grained DB access control for privacy protection
- Flexible and Denial of service resilient ATN approach
- Better understanding of security analysis and constraints in RBAC
- Build an RBAC (ESM) server
  - probably based on directories



Next Lecture

- Student final project presentations