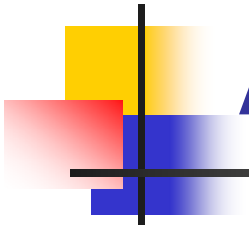
CS590U

Access Control: Theory and Practice

Lecture 2 (Jan 13)

Overview of Project Topics



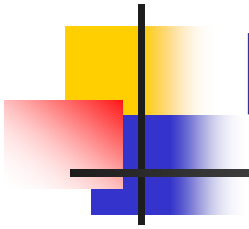
Announcements

- Mailing list
  - CS590U_Spring2005@cs.purdue.edu
  - To join: send email to mailer@cs.purdue.edu
    - with the following in the email body
      add your_email to CS590U_Spring2005
  - Join by Friday the end of the day!

Please fill out index cards

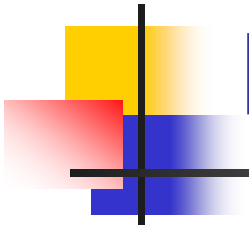
- Name
- Preferred name
- Email address
- Taking or auditing
- Which department/program
- Which year

My Projects



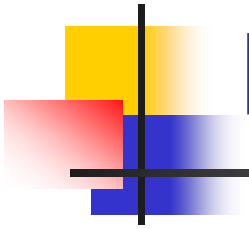
NSF ITR

- Title & dates:
  - Automated Trust Negotiation in Open Systems
  - September 2003 to August 2008
- Joint project with BYU, GMU, UIUC, Stanford
- My activities
  - Continue developing more sophisticated TM languages and evaluation algorithms
  - Developing cryptographic approaches to ATN



Research Goals

- Development of an access control policy language that simultaneously supports credentials with internal structure, pseudonymous credentials, credentials representing delegation and more complex relationships between entities, certain nonmonotonic constructs such as revocation checks, and entities acting jointly to achieve access;
- Design and implementation of light-weight policy evaluation engines for these and additional proposed language features

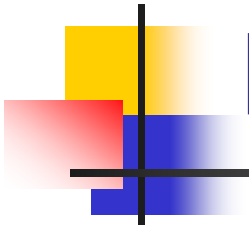


Research Goals

- Improved negotiation protocols and strategies compatible with these new language features and that provide provably stronger privacy guarantees regarding leakage of information and protection of sensitive policy content, as well as strong provisions for autonomy in parties' choice of negotiation strategies;
- The investigation of radically different approaches for trust negotiation that rely on new cryptographic techniques;
- Algorithms and tools for policy analysis

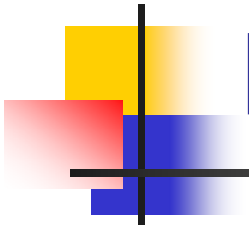
NSF Cyber Trust

- Title & dates
  - Collaborative Research: A Comprehensive Policy-Drive Framework For Online Privacy Protection: Integrating IT, Human, Legal and Economic Perspectives.
  - October 2004 to September 2007.
- Joint project with NCSU



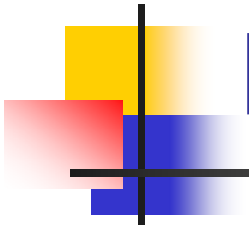
Main research goals

- Research Goal 1: Develop a formal language for specifying privacy policies.
- Research Goal 5: Develop a policy language for specifying access control and auditing policies.
- Research Goal 6: Develop theory and tools for comparing top-tier and middle-tier policies.
- Research Goal 7: Develop theory and tools for comparing top-tier and middle-tier policies.
- Research Goal 9: Understand users' privacy concerns and goals.
- Research Goal 10: Develop a paradigm for specifying privacy preferences.
- Research Goal 11: Develop and evaluate methods and tools to present privacy policies to end users in a uniform and accessible way.



NSF CAREER

- Title & dates:
  - CAREER: Access Control Policy Verification Through Security Analysis And Insider Threat Assessment

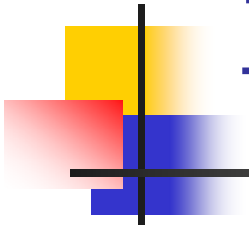


Research Goals

- novel formulations of the security analysis and insider threat assessment problems so that technical measures can be developed to enable administrators to better understand their policies and to effectively analyze and mitigate insider threats;
- new algorithms, computational complexity results, and tools for security analysis and insider threat assessment in RBAC
- a new scheme to improve RBAC administration by supporting controlled delegation of administrative privileges and separation of duty;
- novel verification techniques and tools for enterprise authorization management systems; and
- general techniques and methodologies for access control policy verification applicable to other access control models.

Overview of Course Project Topics

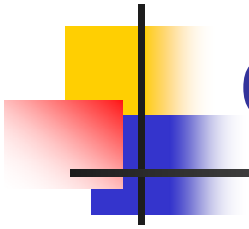
1: Usability study of two approaches for specifying firewall policies



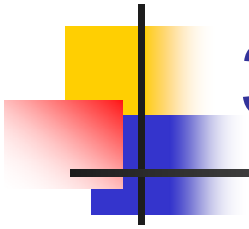
- Comparing the usability of two approaches for specifying filtering policies for a single firewall:
  - (1) the standard approach based on a sequence of rules and
  - (2) firewall decision diagrams, which were proposed recently by Alex Liu and Mohamed Gouda at UT Austin.

- The activities would involve designing a usability study protocol (e.g., problems to ask human subjects to do), run the experiment with human subjects, and analyze the data. This project will be carried in collaboration with Alex Liu at UT Austin.

2: Access control to data stored on smart cards



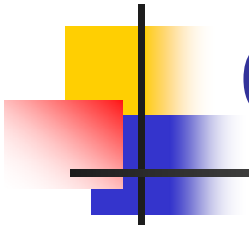
- Store information that have different access control requirements on a smart card and protect the access to such data. The direct motivation comes from designing a medical smart card. Some information on the card may be accessed by everyone; some information may be accessed only by readers with certain properties; some may be accessed only when a secret PIN is inputted to the reader by the user. This project will design these mechanisms and implement them with actual smart cards.
- A second step is to integrating the above with using smart cards as authentication and access control tokens.



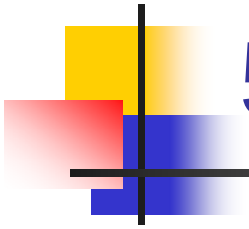
3: Privacy-centric access control

- Traditional Discretionary Access Control has the notion of owners. In privacy-centric access control, there are various party who should have some level of control of the data, for example, data subjects (the persons whose data are stored), data collectors (the entities who collected the information), and data creators (the entities who created the data). It would be interesting to analyze the relationships among these and other parties and come up with a language to document such relationships and determine whether data uses are authorized or not. The starting point for relevant literature includes P3P, XrML, and a paper by Carl Gunter et al. in PET 2004.

4: LDAP Enterprise Access Control Server



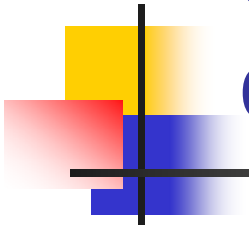
- The goal of this project is to implement a Role-Based Access Control system for enterprises using a LDAP (Lightweight Directory Access Control) server.



5: Access Control in Healthcare

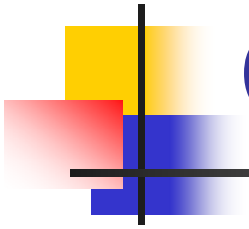
- The goal of this project is to survey access control requirements and existing work on access control in Healthcare systems. A list of 15+ research papers and articles will be provided by the instructor. The student is expected to read most of these documents as well as to conduct additional literature research.

6: Access Control in Workflow Systems and computer supported collaborative work systems

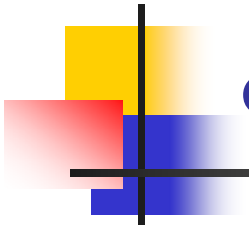


- The goal of this project is to survey access control requirements and existing work in workflow systems and computer supported collaborative work (CSCW) systems. A list of 15+ research papers and articles will be provided by the instructor. The student is expected to read most of these documents as well as to conduct additional literature research.

7: Access Control in SQL and Oracle



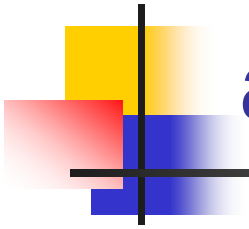
- Clearly describe all the access control features in SQL and how they interact
  - grant/revoke, columns, views, (update), stored procedures, roles
- Clearly describe all the access control features in Oracle
  - in addition to the above, VPD
- Study the differences between standard SQL and Oracle
- Identify tricky effects of access control features interacting with each other



8: Adding Access Control to RMI & EJB

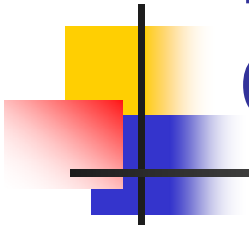
- Building on my previous work “Securing Java RMI-based Distributed Applications”
- Goals:
  - Understanding how RMI security affects EJB
    - how to break EJB applications based on insecurity of RMI
  - How to make applications secure by automatically changing the code

9: A formal model for enterprise authorization management (Ji-won)

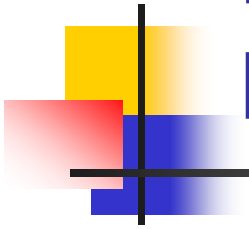


- Enterprise authorization management (EAM) systems have been increasingly popular, because of their ability to deal with complicated requirements of managing large number of employees and diversified resources. While most EAM systems use some elements of RBAC; they all add extensions that go significant beyond RBAC, because of some of the inherent limitations of RBAC. However, these extensions are often ad-hoc and sometimes imprecisely specified. This project aims at coming up an access control model suitable for enterprise authorization model.

10: Automated Trust negotiation with OACerts (Jiangtao)



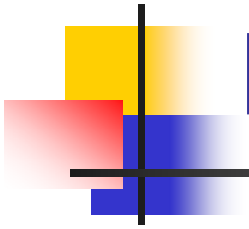
- Traditional ATN approaches use only access control techniques and view a certificate as a blackbox object. Oblivious Attribute Certificates (OACerts) enable one to take advantage of the fact that a certificate is a cryptographic object and introduce many more powerful ways of using attribute values through cryptographic protocols, while revealing limited information about these attribute values. This project aims at coming up with a comprehensive framework for integrating these cryptographic capabilities into access-control based ATN protocols.



11: Insider threat assessment in Role-Based Access Control (Qihua)

- This project designs and implements insider threat assessment algorithms in RBAC. The insider threat assessment analyzes which colluding malicious administrators can do certain damages in an RBAC system. This project will implement two search algorithms in XSB and compare the performance of the two approaches.

- Send me emails or see me if you want to know more about a particular topic and just talk about possible topics
  - If you have specific questions, ask them.



End of Lecture 2

- Next lecture:
  - State-Transition Systems
  - The Granham-Denning DAC schemes