

# CS590U

## Access Control: Theory and Practice

Lecture 1 (August 26)  
Introduction and Overview of  
Projects

## Instructor Info

- Ninghui Li
  - Email: [ninghui@cs.purdue.edu](mailto:ninghui@cs.purdue.edu)
  - Office phone: 765-464-8519
  - Office: REC 217C
- Office hour
  - Tuesday 3pm to 4pm
  - Wednesday 2pm to 3pm
  - Thursday 3pm to 4pm

2

## Please fill out index cards

- Name
- Preferred name
- Email address
- Taking or auditing
- Which department/program
- Which year
- Graduate-level security courses
- Advisor

3

## Coursework

- One homework November 4 10%
- A course project
  - Pre-proposal Sep 4
  - Project proposal due Sep 30 20%
  - Lecture Oct/Nov 20%
  - Mini defense Dec 15%
  - Final report Dec 16 35%

4

## Pre-proposal (Due Sep. 4) Submit paper copy before class

- List 2 to 4 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 ...

5

## 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.

7

## Access Control is Useful

- Access control is Pervasive
  - OS (Unix, Windows), Databases, Java, Firewall, Middleware
- Quote from Security Engineering
  - Access control is the traditional center of gravity of computer security. It is where security engineering meets computer science.

8

## Access Control is Interesting

- Has (relatively) well-developed theory
  - 30+ years history
- Big gap between theory and practice
  - Potential fruitful future research areas
    - policy management and analysis
    - human factors
- No standard textbook/course exists

9

## 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

10

## Principles of Access Control

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

11

## 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

12

## 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

13

## Project Ideas (For Details, See Syllabus)

- Evaluating the Effectiveness of Access Control in SELinux.
- Static Analysis for Determining A Program’s Access Requirements.
- Fine Grained Access Control in Databases.

14

## Human Factors in Access Control (Also see Syllabus)

- Understand usability evaluation
  - how to set up tests
  - how to interpret results
- Books
  - Usability Engineering (by Jakob Nielsen)
  - Human-Computer Interaction in the New Millennium (edited by John Carroll)

15

## Project Ideas Related to Firewalls

- Idea one
  - high-level language to hide low-level trickiness
  - from Inside Network Perimeter Security by Stephen Northcutt, et al.
- Idea two
  - central management and analysis of firewall policies
  - from several previous projects

16

## Backgrounds on Trust Management

## What is Trust Management?

- An approach to decentralized access control
  - principals can make statements
  - access control decisions are based on statements made by multiple principals
- Common characteristics of TM systems:
  - treat public keys as principals
  - use digitally signed credentials

18

## What One Can Express in $RT_0$

- B says that D is a student
- A says that B is a university
- A believes that someone is a student if a university says so
- C says that D is an ACM member
- A grants access to X to anyone who A believes is a student and C believes is an ACM member

19

## What One Can Express in $RT_1$

- B says that D is a student that has name ..., department ..., year ...
- A says that only students of certain years and certain departments can do ...

20

## What One Can Express by Adding Constraints to $RT_1$

- A says that B can admin any host in a domain purdue.edu
- B says that D can access any host in the domain cs.purdue.edu
- D wants to access arthur.cs.purdue.edu
- A should give D access
- Semantic foundation: Constraint Datalog

21

## What Queries One Can Ask

- Is D authorized access X?
- Who can access X?
- What can A access?
- If someone is not fully trusted, what could happen in the future.

22

## Automated Trust Negotiation

- A and B each has a set of credentials; they want to exchange credentials to establish trust, but they also consider their credentials to be sensitive
- Automated Trust Negotiation

23

## End of Lecture 1

- Pre-proposal due Thursday next week (Sep 4)
- Welcome to meet with me to discuss project ideas
- Security reading group meet this Wednesday
  - join the mailing list security-reading-group from cs.purdue.edu machines

24