Data Security and Privacy Course Overview

Purdue University

Prof. Ninghui Li

Planned Topics

- Access control (AC)
  - Operating system AC, mandatory AC, discretionary AC, role based AC, attribute-based AC, non-interferences, integrity protection, firewall policy languages, AC in databases, AC in mobile systems, AC in web
- Using crypto for data protection
  - Implementing crypto correctly, Authentication protocols, Homomorphic encryption, secure multiparty computation
  - Using SGX and hardware security architectures
- Data privacy
  - Privacy policies, data anonymization (k anonymity, t closeness, l diversity), differential privacy: concepts and algorithms, differential privacy in the local setting, membership privacy

Relationship to Other Security Courses

- Require basic knowledge from
  - 526 Information Security
  - 555 Cryptography
- Little overlap with
  - 527 Software Security
  - 528 Network Security
  - 523 Social Econ Legal Asp Of Sec
  - 529 Security Analytics

Logistics

- Time and location: TTh 3:00-4:15pm, HAAS G066
- Instructor: Ninghui Li <ninghui@purdue.edu>,
  - LWSN 2142K, office hours: After lecture and Mondays 3:30
- Teaching assistants: Huangyi Ge <geh@purdue.edu>
  - LWSN 2161, office hours, TBA
- Webpage: http://www.cs.purdue.edu/~ninghui/courses/Spring18
- Piazza signup: piazza.com/purdue/spring2018/cs590

Readings

- No required text, readings will be announced/distributed on course webpage.

- Reading for this lecture:
  - Part 1A of Saltzer and Schroeder: “The Protection of Information in Computer Systems”.

Workload

- Homeworks
  - About 6 assignments, which will be either written assignments, or small projects that require programming
  - Late policy: Five extension days to be used at your discretion
    - Must be stated explicitly in header of work being turned in
    - No fractional days
    - May not be used to extend submission past last day of class.
- Exams
  - 4 (in-class) quizs during the semester
  - Mid-term exam
  - Final exam

Policies for Homework Cheating

- It is allowed/encouraged to discuss homework problems
- However, if you looks at another student's written or typed answers, or let another student look at your written or typed answers, that is considered cheating.
- If caught for the first time, receive 0 in the assignment. For the second time, receive a failing grade in class.

EMERGENCY PREPAREDNESS – A MESSAGE FROM PURDUE

To report an emergency, call 911. To obtain updates regarding an ongoing emergency, sign up for Purdue Alert text messages, view www.purdue.edu/ea.

There are nearly 300 Emergency Telephones outdoors across campus and in parking garages that connect directly to the PUPD. If you feel threatened or need help, push the button and you will be connected immediately.

If we hear a fire alarm during class we will immediately suspend class, evacuate the building, and proceed outdoors. Do not use the elevator.

If we are notified during class of a Shelter in Place requirement for a tornado warning, we will suspend class and shelter in [the basement].

If we are notified during class of a Shelter in Place requirement for a hazardous materials release, or a civil disturbance, including a shooting or other use of weapons, we will suspend class and shelter in the classroom, shutting the door and turning off the lights.

Please review the Emergency Preparedness website for additional information.
http://www.purdue.edu/ehps/emergency_preparedness/index.html

Some Recent Data Breaches

- Equifax 2017
- Anthem 2015
- Target 2014
- Yahoo 2014
- Adobe 2013

Some Recent Privacy Incidents

- Sony CD Spyware
- Samsung smart TV snooping
- Many more

AOL Data Release [NYTimes 2006]

- In August 2006, AOL Released search keywords of 650,000 users over a 3-month period.
  - User IDs are replaced by random numbers.
  - 3 days later, pulled the data from public access.

AOL searcher # 4417749
"landscapers in Lilburn, GA" *queries on last name "Arnold"* *"homes sold in shadow lake subdivision Gwinnett County, GA"* *"num fingers"* *"60 single men"* *"dog that urinates on everything"*

NYT

Thelman Arnold, a 62 year old widow who lives in Liburn GA, has three dogs, frequently searches her friends' medical ailments.

Re-identification occurs!

What is Information (Computer) Security?

- Security = Sustain desirable properties under intelligent adversaries
- Make the above precise requires making the following two precise

- Desirable properties
  - Understand what properties are needed.
- Intelligent adversaries
  - Needs to understand/model adversaries
  - Always think about adversaries.

Security Goals/Properties (C, I, A)

- Confidentiality (secrecy, privacy)
  - only those who are authorized to know can know
- Integrity (also authenticity in communication)
  - only modified by authorized parties and in permitted ways
  - do things that are expected
- Availability
  - those authorized to access can get access

What is Privacy?

It is complicated! Privacy is primarily a social and legal concept.

Some concepts from the book "Understanding Privacy" by Daniel J. Solove:

1. the right to be let alone
2. limited access to the self
3. secrecy—the concealment of certain matters from others;
4. control over others' use of information about oneself
5. personhood—the protection of one's personality, individuality, and dignity;
6. intimacy—control over, or limited access to, one's intimate relationships or aspects of life.

Security is Secondary

- What protection/security mechanisms one has in the physical world?
- Why the need for security mechanisms arises?
- Security is secondary to the interactions that make security necessary.

Robert H. Morris: The three golden rules to ensure computer security are: (1) do not own a computer; (2) do not power it on; and (3) do not use it.

Information Security is Interesting

- The most interesting/challenging threats to security are posed by human adversaries
  - Security is harder than reliability
- Information security is a self-sustaining field
  - Can work both from attack perspective and from defense perspective
- Security is about benefit/cost tradeoff
  - Thought often the tradeoff analysis is not explicit
- Security is not all technological
  - Humans are often the weakest link

Information Security is Challenging

- Defense is almost always harder than attack.
- In which ways information security is more difficult than physical security?
  - adversaries can come from anywhere
  - computers enable large-scale automation
  - adversaries can be difficult to identify
  - adversaries can be difficult to punish
  - potential payoff can be much higher
- In which ways information security is easier than physical security?

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 Security/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 Security/Access Control

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

Principles of Security/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 Security/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 Domains

- Workflow systems
- Firewall
- Mobile systems

Readings for Topic 1

- Saltzer and Schroeder . The Protection of Information in Computer Systems