Overview: CS 5432

Spring 2021

Fred B. Schneider

Samuel B Eckert Professor of Computer Science

Department of Computer Science
Cornell University
Ithaca, New York 14853
U.S.A.

Today's Agenda

- Course content
- Organizational matters

Content: Big Picture

- CS 5430: Principles and mechanisms in use **today**.
  - These address a need that exists today.
  - These are available in systems that exist today.

- CS 5432: Mechanisms, policies, and analysis not in use today but **likely to be used within a decade**.
  - Will enable transition from craft → engineering discipline.
  - Avoid ad hoc simplifications (about trust and policy).
  - (Basis for startups and new product offerings).

Future: Threat stays the same

… but the targets of attack change in the future.

- Greater use of COTS in critical public infrastructure.
  - Power grid, communications, …
- More societal dependence on commercial infrastructure.
  - E.g. google's gmail, …
- Advent of smart "things" (some can kill).
  - E.g. cars
- New societal sensibilities → new policies.
  - Privacy, fairness, mis-information, accountability

… today's "military grade" security (mechanisms and policies) will be needed and used in tomorrow's commercial settings.

CS5432 Content Overview

Gold Standard

- Authentication
- Authorization
- Audit

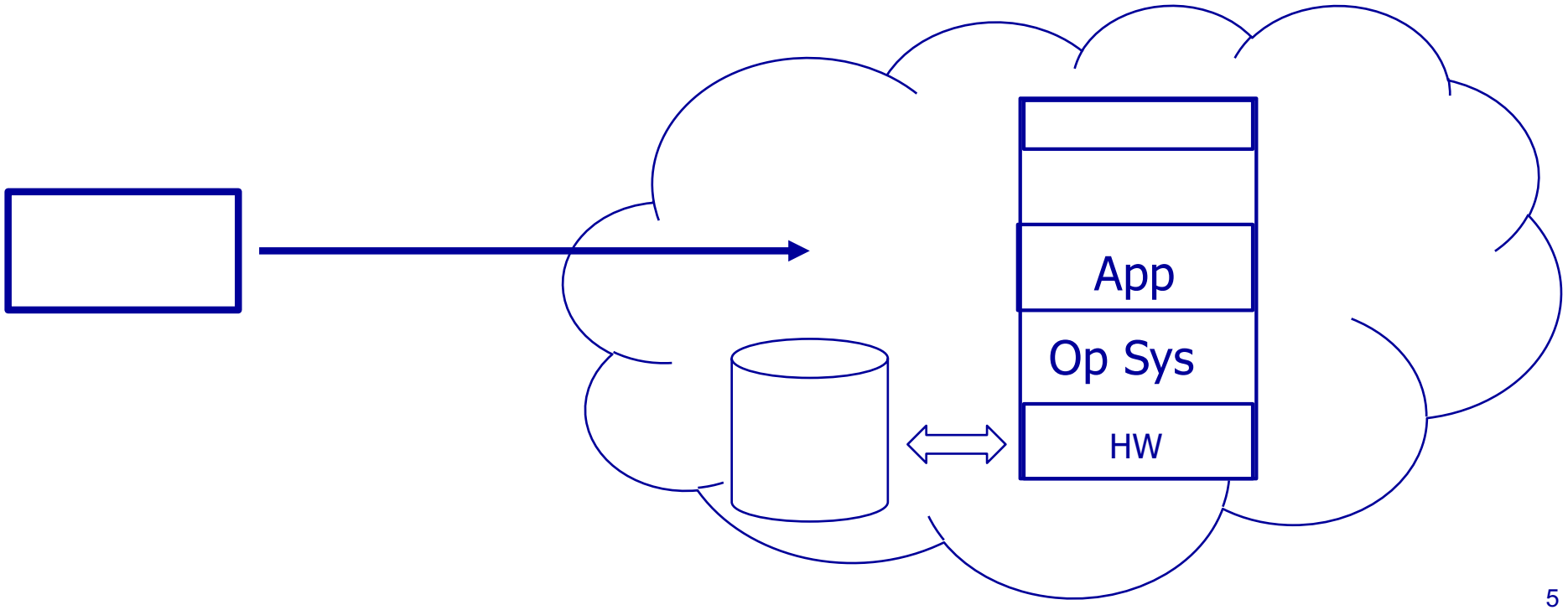
Defenses

- Isolation
- Monitoring
- Independence
- Asymmetric Work

Authentication of Things

"Easy" if there is a shared secret…

- What principal stores the secret for a "thing"?
- What principals must be trusted?



Authentication of Things: Topics

- Authentication of inanimate objects
  - Paper money, other objects, chips, …
- PUFs (to authenticate an IC)
- Measured principals and gating functions
  - HW support (TPM)
  - Remote attestation protocols
- Use of **says**/**speaksfor** for specifying and reasoning about trust assumptions and consequences.

Authorization: Information Flow

Access control associated with

- object (DAC vs MAC) -vs-
- content (information flow)

Information flow "solves"

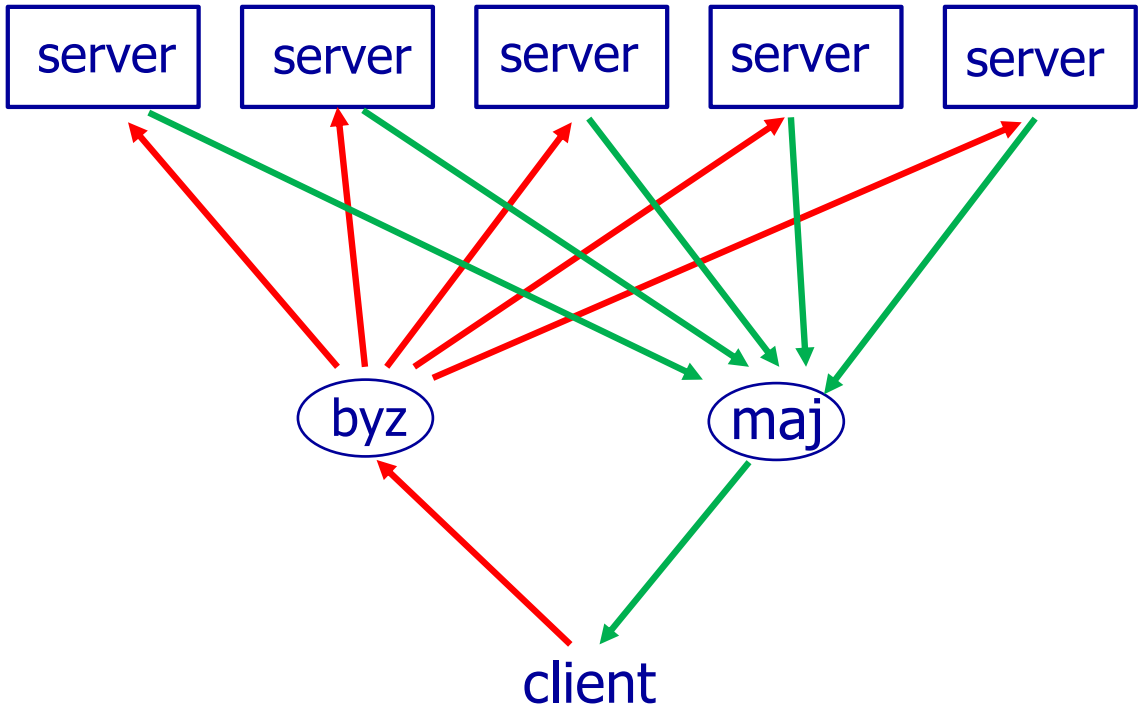
- spectre/meltdown + other side channels
- *actual* confidentiality / integrity

Information Flow: Topics

- Lattice-based policies
- Enforcement
  - static
  - dynamic
  - reclassification
- Other flow policies
  - semantics of flow
  - verification of flow policies

Independence

- Replication for fault-tolerance
- = Replication for attack-tolerance?



Independence: Topics

- Support for independent replicas
  - secret sharing and threshold cryptography
  - proactive secret sharing
  - proactive code obfuscation
- Moving target defenses

Execution Assumptions

- Control flow
  - Attacks (buffer overflow, ROP)
  - Defenses (CFI/XFI)
- Memory
  - Attacks
  - Defenses (memory safety)

CS5432
Administration

Course Staff

Fred B. Schneider

- fbs@cs.cornell.edu

Natalie Neamtu

- nan55@cornell.edu

Content Delivery

Lectures: Mon and Wed 2:40 – 3:30pm

- By zoom. Plan to attend, live.
- Recordings avail for review afterwards.

Readings: Will be added to course outline as semester progresses.

- Suggestion: Do the reading after the lecture.

Office Hours:

- Drop-in (=not private) scheduled Mon - Thurs.
- Send email to FBS for individual meetings.

Learn by Doing

- Written Homework (30%)
  - Opportunity to exercise what you have learned.
- Project (50%)

  Implement a social networking system.
    - Authentication of people, of machines, authorization of access, confidentiality of content
    - Work in groups
    - Multiple phases
    - Presentation and demo last 2 weeks
- Other inputs to grade (20%)
  - Extra-credit HW assignments
  - Class attendance and participation
  - Other engagement with course content

Nota bene

- Letter grade only (no S/U)
  - Avoids odd dynamics in groups
- Academic integrity.
  - It matters and will be enforced.
  - Source and sink of collaboration both are in violation.

Truth in Advertising

- New course
  - New lectures (presentation undebugged)
  - New content (understanding undebugged)
  - New homeworks (but project is not new ☺)
  - Course staff learning, too
- Logic and formalism alert

$$\neg P \wedge (P \Rightarrow Q) = \neg P \ ?$$

  - We will do a review…

Equational Proof ….

$\neg P \wedge (P \Rightarrow Q)$

= ⟨ defn of ⇒: Implication Laws (2.22a)⟩

$\neg P \wedge (\neg P \vee Q)$

= ⟨ distribution of ∧ over ∨: Distributive Laws (2.16b) ⟩

$(\neg P \wedge \neg P) \vee (\neg P \wedge Q)$

= ⟨ identity of ∧: And-Simplification Law (2.26a) ⟩

$(\neg P) \vee (\neg P \wedge Q)$

= ⟨ absorption. Or-Simplification (2.25d) ⟩

$\neg P$