CS 334: Computer Security

Spring 2026

Website:

c334-spring-2026.github.io

A good reference text:
Computer Security and the Internet: Tools and Jewels by Paul Van Oorschot

Thanks to Paul for many of the definitions and related info throughout the course.

Thanks also to Anthony Joseph, Doug Tygar, Umesh Vazirani, and David Wagner of the University of California, Berkeley, for their generosity in allowing me to use some of their course material (slides and handouts)

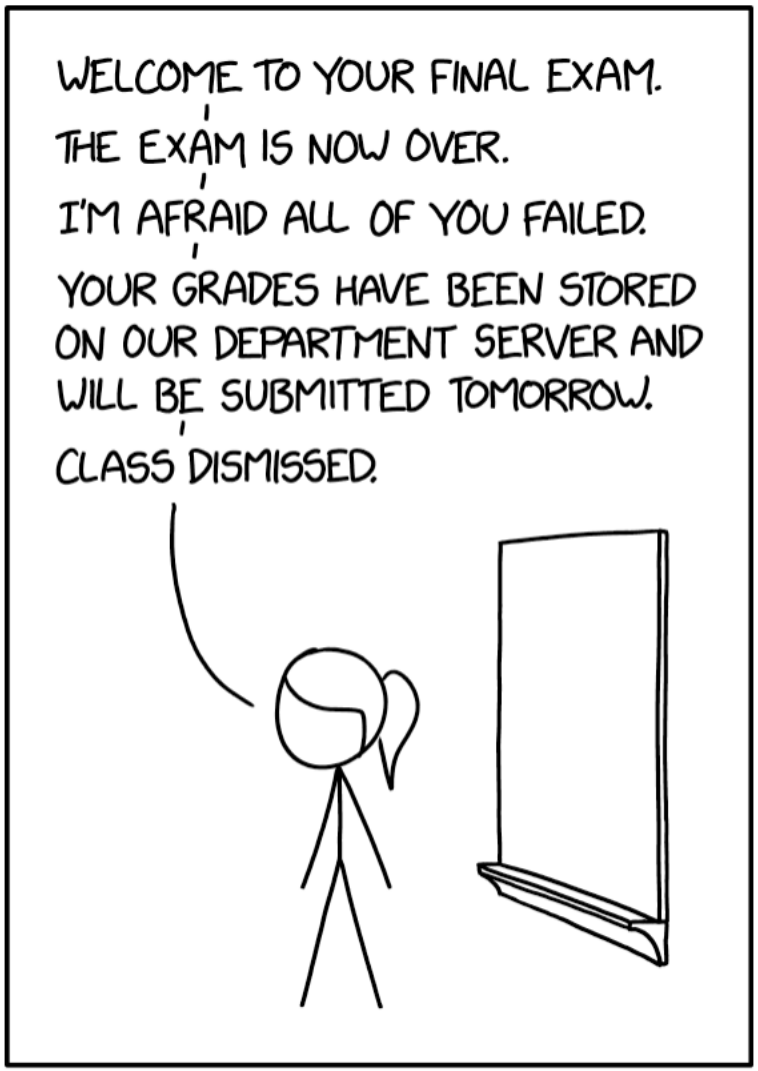
Goals of this class

- Solid foundation in understanding security
- Key information a/b building secure systems
- Introduce range of topics in security
- Interest some of you in further study

Introduction

Attacks

Security Goals



CYBERSECURITY FINAL EXAMS

What is Computer Security?

The combined art, science and engineering practice of protecting computer-related assets from unauthorized actions and their consequences, either by preventing such actions or detecting and then recovering from them.

P. Van Oorschot

- In practice: Risk analysis and management!
  - As we will see, you cannot prevent all such malicious actions
  - So we try to make the actions more costly than the reward

What is Computer Security?

The combined art, science and engineering practice of protecting computer-related assets from unauthorized actions and their consequences, either by preventing such actions or detecting and then recovering from them.

P. Van Oorschot

- Note that the goal here is to protect computer-related assets from *intentional* misues by unauthorized parties.
- Studies of reliability, redundancy, and fault-tolerance consider questions of *unintentional* damage of mistakes.
- So effectively, the existence and capabilities of a malicious *adversary* is a necessary consideration

Why Is Security Such a Problem?

- Existence of monoculture computing environments
- Web, e-commerce, & collaborative applications
- Internet spans national boundaries
- Poor programming practices
- Inherently more difficult to defend vs disrupt

Security Goals

- **Confidentiality**: The property of non-public information remaining accessible only to authorized parties, whether stored (at rest) or in transit (in motion).
  - Sometimes called privacy
  - *Encryption* is one means for achieving this
    - There are others, e.g., physical security
  - Can sometimes apply to existence of data

Security Goals (cont.)

- **Integrity**: The property of data, software or hardware remaining unaltered, except by authorized parties
  - Sometimes people speak of trustworthiness of data or resources.
  - Typically refers to preventing improper or unauthorized modification

Security Goals

- **Availability**: the property of information, services and computing resources remaining accessible for authorized use.
  - A so-called *denial-of-service attack* is an attack on availability

Security Goals

- **Authentication**: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. (*NIST Computer Security Resource Center*)

- Sometimes people call this origin integrity
  - As opposed to data integrity

Integrity

- Example: the correct quote credited to the wrong source preserves data integrity but not origin integrity.

Security Goals

- **Accountability**: the ability to identify principals responsible for past actions.
  - As the electronic world lacks conventional evidence (e.g., paper trails, human memory of observed events), accountability is achieved by transaction evidence or logs recorded by electronic means, including identifiers of principals involved, such that principals cannot later credibly deny (repudiate) previous commitments or actions.

A Note on Confidentiality

- All confidentiality enforcement mechanisms require supporting services from system.
  - Assumption is that security services can rely on kernel and other agents, to supply correct data. Thus *assumptions* and *trust* underlie confidentiality mechanisms.
- **Confidentiality is not integrity**
  - Just because an attacker can't read it, doesn't mean they can't change it!

Integrity

- Two classes of mechanisms
  - **Prevention** mechanisms: maintain integrity by blocking unauthorized attempts to change data or by blocking attempts to change data in unauthorized ways.
  - **Detection** mechanisms: report that data's integrity is no longer trustworthy

More on Integrity

- Affected by
  - Origin of data (how and from whom it was obtained)
  - How well data protected before arrival at current machine
  - How well data is protected on current machine
- Evaluating is difficult: relies on assumptions about source and about trust in that source

Availability

- Relevant to security because someone may be attempting to affect data or service by making it unavailable
  - Ex. Some software (e.g. network code) depends for correct operation on underlying statistical information and assumptions. By changing, for example, service request patterns, an adversary can cause this code to fail.

Availability

- Attack on availability is called a *denial of service* attack
  - Difficult to detect: is it a deliberate phenomenon or just an unusual access pattern? Also, even if underlying statistical model is accurate, atypical events do occur that may appear to be malicious!
  - Distributed denial of service is particularly pernicious

Threat Related Terminology

- I'll be giving you a number of terms
  - I won't test you on them, but I will use them
  - So if I use one, and you don't remember what it is…

Threat Related Terminology

- Vulnerability: Weakness (in security system) that might be exploited to cause loss or harm.
- Threat: Set of circumstances that has potential to cause loss or harm
- The difference?
  - Losing important file is a threat. The weakness in the system that allows this is the vulnerability

Threat Related Terminology

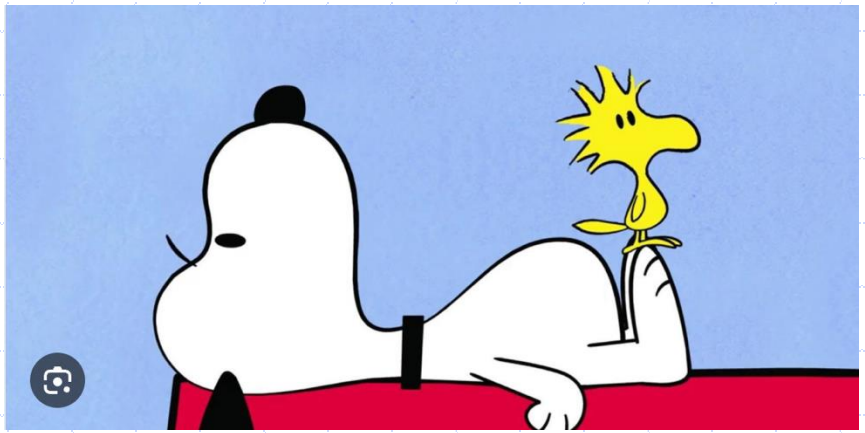
- Attack: actions that could cause violation to occur
- Attacker: those who cause such actions to be executed
- Passive attack: attacker merely observes (e.g., traffic analysis)
- Active attack: attacker actively modifies data or creates false data stream

Examples and Terms

- Snooping: unauthorized interception of information (form of disclosure). Countered by confidentiality mechanisms
  - Ex. Wiretapping

Examples and Terms

- Snooping: unauthorized interception of information (form of disclosure). Countered by confidentiality mechanisms
  - Ex. Wiretapping



Examples and Terms

- Modification or alteration: unauthorized change of information
  - Ex. Active wiretapping
  - Ex. Person-in-the-middle attack: attacker reads message from sender and forwards (possibly modified) message to receiver.
    - Countered by integrity and authentication mechanisms

Examples and Terms

- Masquerading or Spoofing: impersonation of one identity by another. Authentication measures counter this threat.

Examples and Terms

- Delegation (one entity authorizes a second entity to perform functions on its behalf)
  - This is a form of masquerading that may be allowed
  - This is not the same as traditional masquerading, since the person performing the action is not pretending to be someone they are not. That is, all parties are aware of the delegation.

Examples and Terms

- Repudiation of origin: false denial that an entity sent or created something
- Denial of receipt: false denial that an entity received some information or message

- Accountability measures counter this
  - You'll see the term non-repudiation

Policy and Mechanism

- Security Policy: a statement of what is, and what is not, allowed
- Security Mechanism: a method, tool, or procedure for enforcing a security policy
  - Mechanisms can be non-technical. Policies often require some procedural mechanisms that technology cannot enforce.

Policies and Mechanisms

- Policies may be presented mathematically, as a list of allowed and disallowed states.
  - In general an axiomatic description of secure states and insecure states
- In practice, rarely this precise
  - Normally written in English, leading to ambiguity (is a state legal or not?)

Policies and Mechanisms

- Policy is not generally considered by most to be "exciting"
  - Or even interesting
  - But it is necessary: If you don't know what actions are authorized, how do you know when unauthorized action(s) occurs?

Assumptions and Trust

- Security rests on assumptions specific to the type of security required and the environment in which it is to be employed.
  - Ex. (Bishop) Opening a door lock requires a key. Assumption is that the lock is secure against lock picking. This assumption is treated as an axiom and made because most people require a key to open a locked door. A good lock picker can, however, open a locked door without a key. Thus in an environment with a skilled, untrustworthy lock picker…

Assumptions and Trust

- Well-defined exception to rules provides a *back door* through which security mechanisms can be bypassed.
  - Trust resides in belief that back door will not be used except as specified by policy.

Assumptions and Trust

- Two assumptions made by policy designers
  - Policy correctly and unambiguously partitions set of system states into secure and insecure states
  - Security mechanisms prevent system from entering an insecure state
  - If either of these fail, system is not secure

Our First Security Principles

- Principle of Adequate Protection:
  - Computer systems must be protected to a degree consistent with their value
- Principle of Easiest Penetration:
  - Count on an intruder to use the easiest means to penetrate the system
  - I.e., System is most vulnerable at its weakest point (regardless of how well other points are defended).