



System Security

EECS 195

Spring 2019

Zhou Li

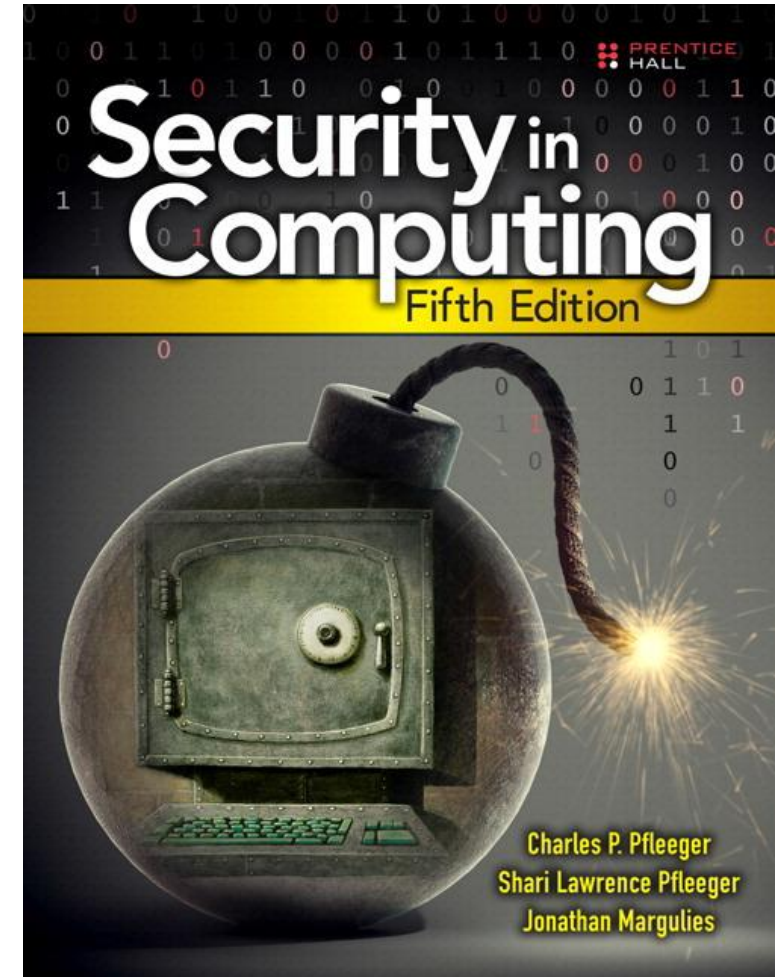


Who am I?

- Zhou (Joe) Li
 - Assistant Professor of Department of Electrical Engineering and Computer Science at UCI (2018-present)
 - Principal Research Scientist at RSA Labs (2014-2018)
 - **Research focus:** system security (focus: data-driven security, Internet measurement, side-channel analysis and IoT security)
- Lectures: **Mon, Wed, Fri 9:00AM - 9:50AM, DBH 1429**
- Office hour: **Mon 3pm-5pm**, by appointment if needed
- Office: 3227 Engineering Hall
- Email: zhou.li@uci.edu

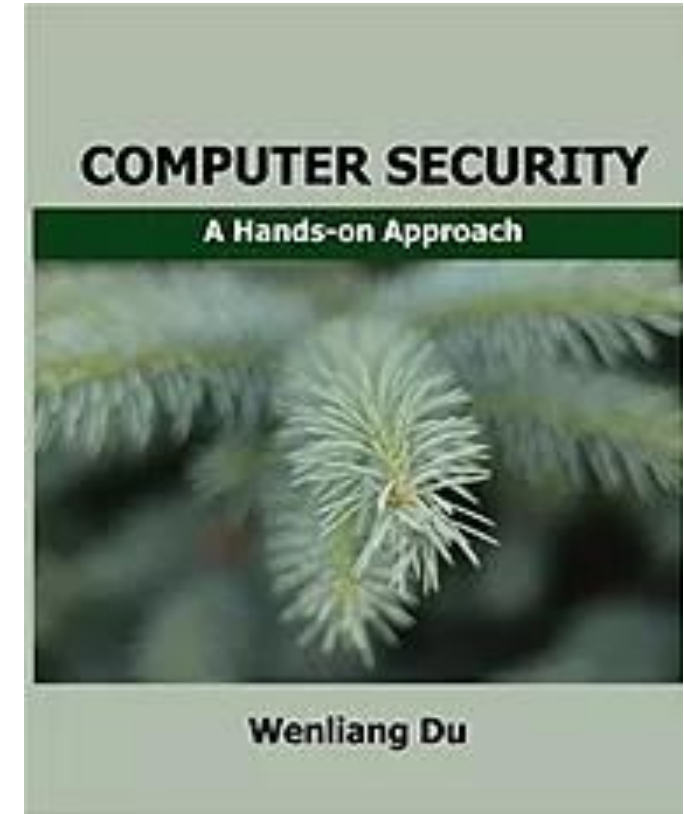
Textbook (required)

- Textbook: Security in computing
 - Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies
 - Publisher: Pearson
 - ISBN-13: 9780134093109
 - 5 edition (February 5, 2015)



Textbook (recommended)

- Textbook: **COMPUTER SECURITY, A Hands-on Approach**
 - Wenliang Du
 - Publisher: CreateSpace Independent Publishing Platform;
 - 1 edition (October 12, 2017)





Course website

<https://canvas.eee.uci.edu/courses/15806>

EECS 195 LEC A: SYSTEM... > Syllabus

Spring 2019

Home

Announcements

Assignments

Discussions

Grades

People

Pages

Files

Syllabus

Outcomes

Quizzes

Modules

Conferences

Collaborations


Attendance

Chat

AEFIS Tools

Settings

EECS 195 LEC A: SYSTEM SECURITY (18280)

Jump to Today 

Instructor:

[Prof. Zhou Li \(Engineering Hall 3227\)](#)

Course Info:

Mon, Wed, Fri 9:00AM - 9:50AM, DBH 1429

Office hour: Mon 3pm-5pm (by appointment if needed)

Prerequisite:

Basic knowledge of OS, network and applications.

Knowledge of programming language, especially C.

The student needs to have a machine that can run virtual machine (Ubuntu 16.04 VM, see [details](#) &).

Course Description:

This course will teach the principles and practices of system security as applied to software-, network-, and hardware-layer. It covers the foundations and techniques of analyzing the security of systems and building secured systems. In addition to the content described by the textbook, the course will also let students have hands-on experiences by playing attacks and defense in an emulated environment.

Main questions to be discussed in this lecture:



Prerequisites

- Basic knowledge of OS (e.g., Linux), network and applications.
- Knowledge of programming language, especially C.
 - UCI EECS courses: **EECS 12** (Introduction to Programming), **EECS 20** (Computer Systems and C Programming), **EECS 22** (Advanced C Programming), **EECS 22L** (Software Engineering Project in C Language)
- The student needs to have a machine that can run virtual machine (**Ubuntu 16.04 VM**).



Expectation

- Complete reading assignment prior to each lecture (textbook chapters and supplemental materials)
- Attend lectures
- Take in-class quiz
- Complete assignments (written and lab-at-home)
 - Discussion is encouraged, but work must be done independently
- Take mid-term and final exams



Grading

Assignment and quiz	45%
Mid-term exam (05/03/2019)	15%
Final exam (06/12/2019 8am-10am)	40%



Policies

- **Assignments** are listed on the "Assignments" page. There are **3 assignments** and the due dates are indicated during lectures.
- **Late policies:** Home work turned in after the due date/time will not be graded and will receive no credit. Make-up assignments can only be arranged for absence due to medical (or similar) reasons. Proper documentation is required.
- **Caveat:** You will have **one** chance (**only one!**) to submit assignment late without asking for permission (no later than 24 hours).
- **Academic Honesty:** Don't cheat. No "github" code.
- Researcher ethics: Hacking **real-world** systems has consequences
 - [E.g., UCI OIT Campus Wide Polices](#)



No class

- Memorial day on **05/27**
- Instructor travels on **04/08, 04/29, 05/20**
 - Mandatory NSF meetings, can't be moved around
 - My apology ☹️
- Potential instructor travel on **06/05 or 06/07**
 - Chair for a workshop
- Options for those missing classes?
 - Video lectures about law & policy chapters (pre-recorded)?
 - Find another time & classroom?

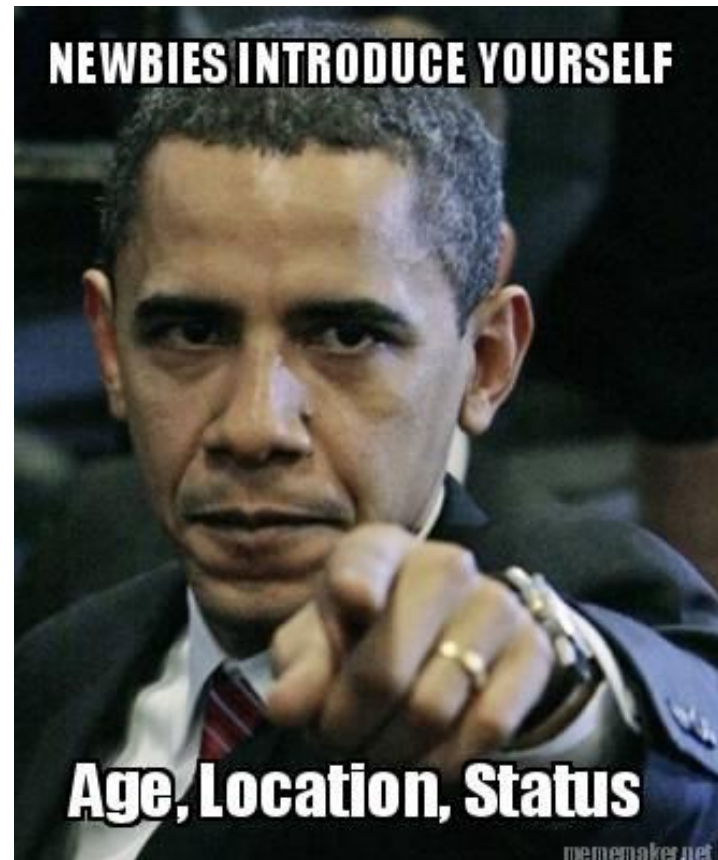


TODO before next lecture

- Fill the survey about no-class option on Canvas
- Install SeedLabs
 - http://www.cis.syr.edu/~wedu/seed/lab_env.html
 - User ID and password
http://www.cis.syr.edu/~wedu/seed/Documentation/Ubuntu16_04_VM/Ubuntu16_04_VM_Manual.pdf
 - Ubuntu 16.04 VM
 - Let me know if you aren't able to do it ASAP

Now let's introduce yourself ...

- Introducing yourself (max 30 seconds)





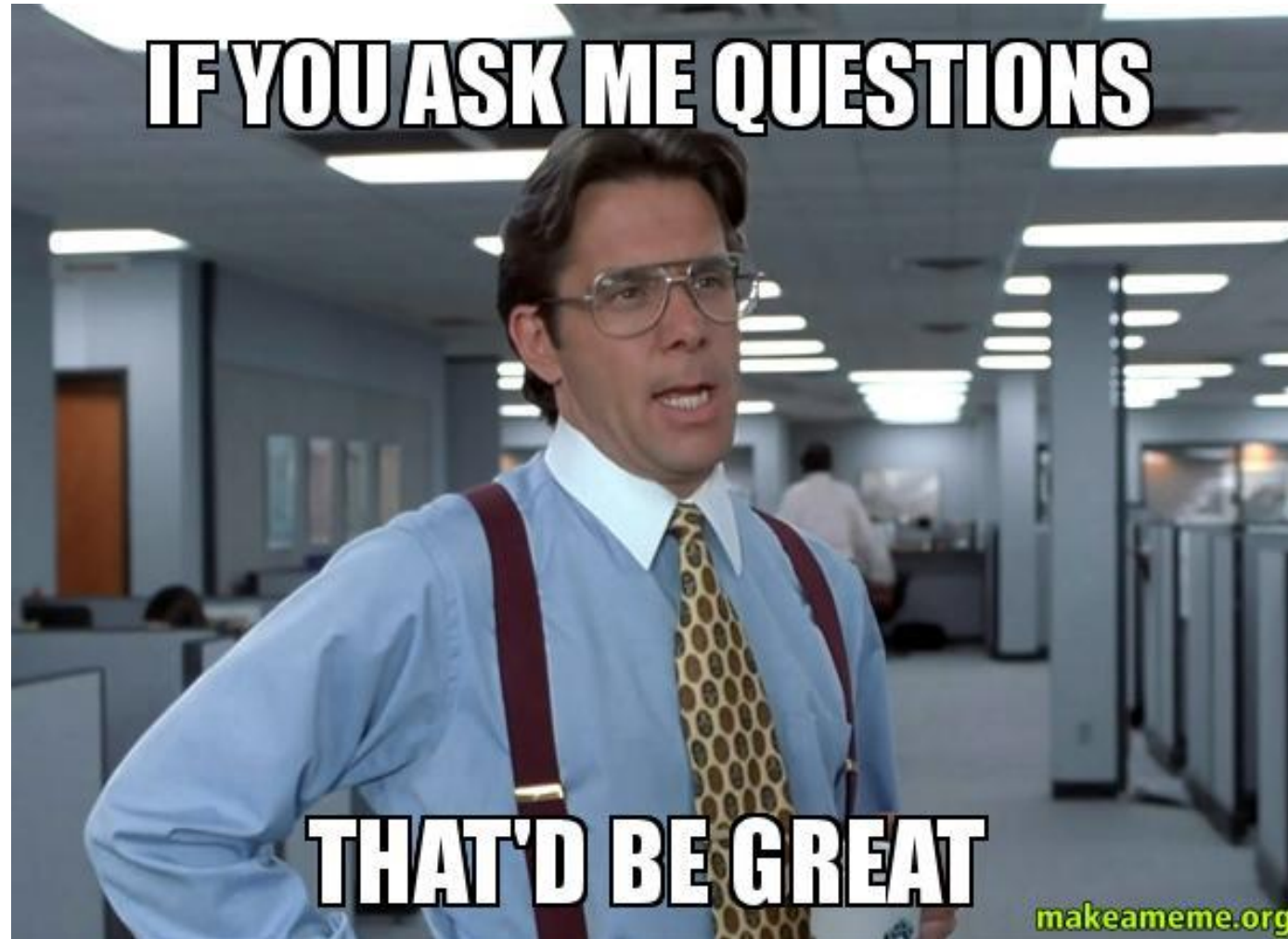
What's covered in this course

- Toolbox (authentication, access control and cryptography)
- Software vulnerabilities and malware
- Web security
- OS security
- Network security
- Database
- Cloud computing
- Privacy
- Legal issues and ethics
- Emerging topics (IoT, electronic voting, ...)
- Hands-on experiences of hacks! (SeedLabs)



Course goals

- When we talk about system security, what are we really talking about?
- What does cyber-attack look like? And how to do it?
- What security techniques are available?
- What principles should we follow to make the systems we build (software/hardware) secure?

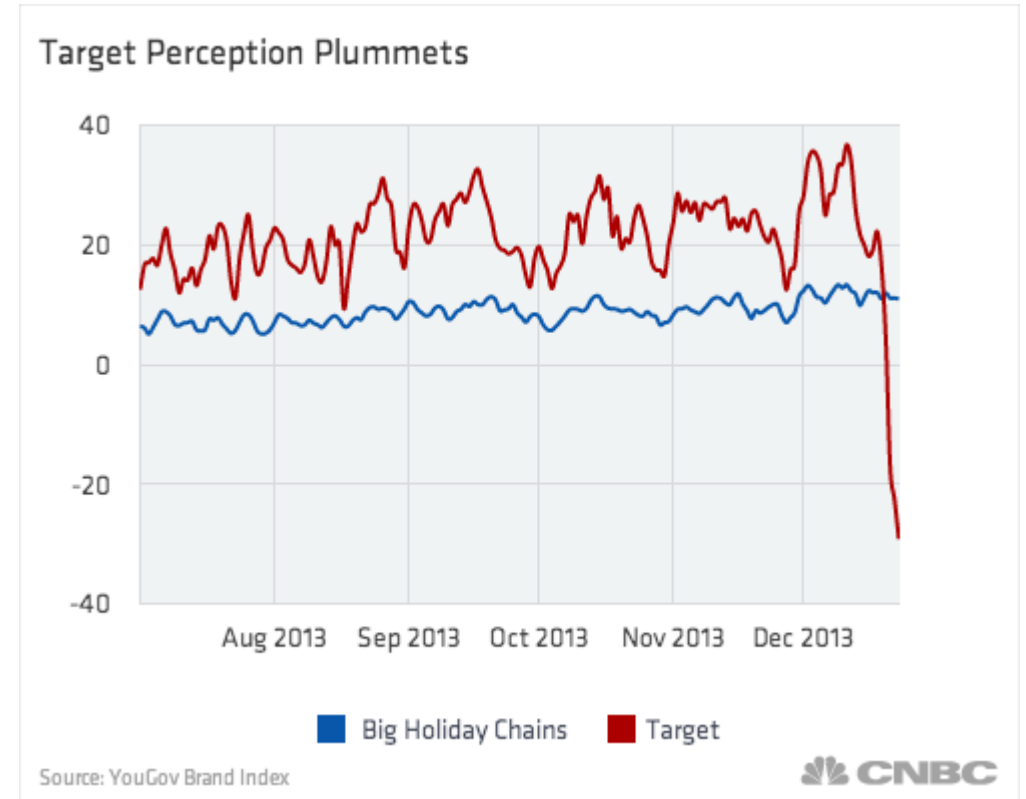




Security fail



Chart of the Day: Target's image takes a beating





What Is Computer Security?

- The protection of the assets of a computer system
 - Hardware
 - Software
 - Data



Assets



Hardware:

- Computer
- Devices (disk drives, memory, printer)
- Network gear

Software:

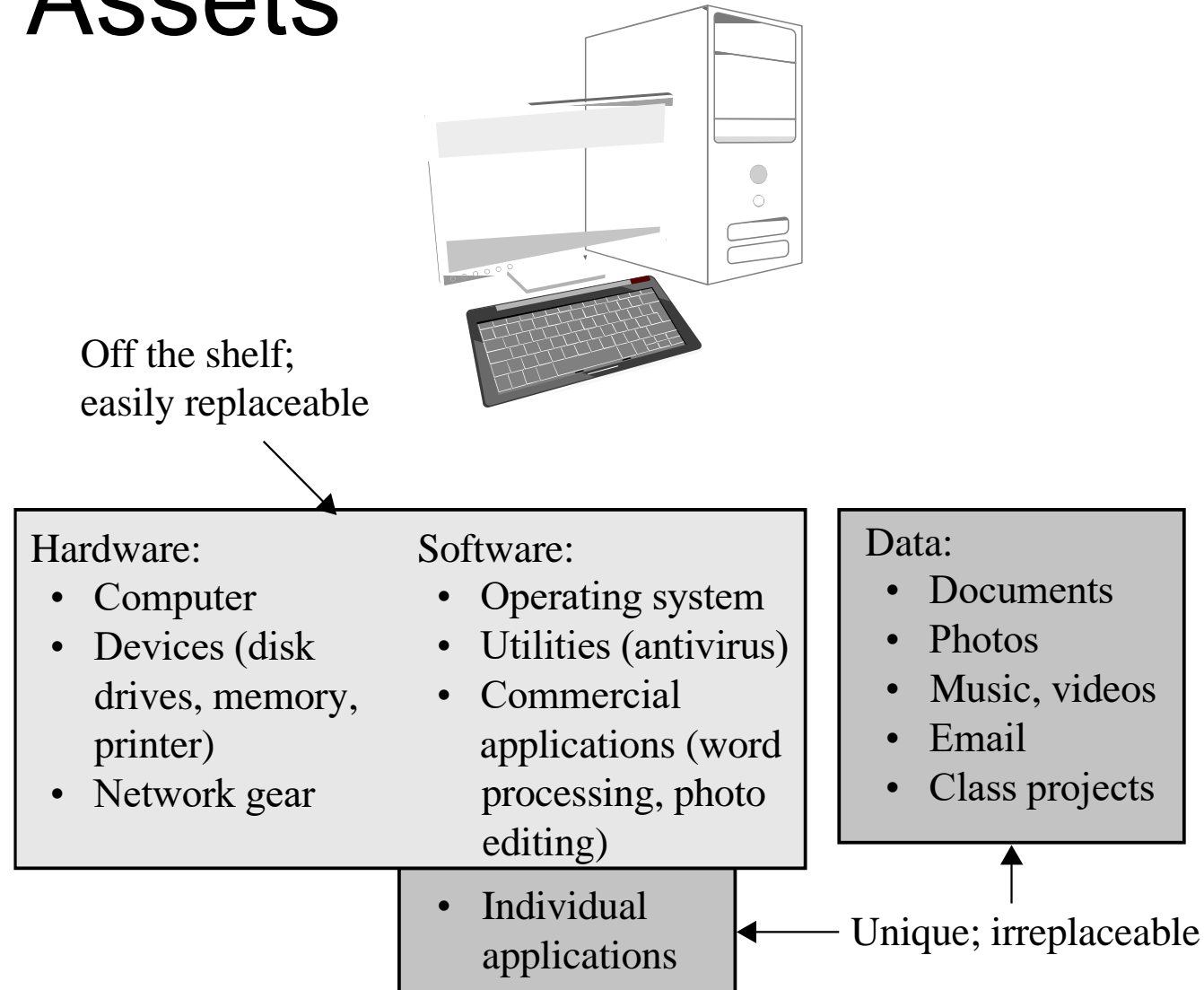
- Operating system
- Utilities (antivirus)
- Commercial applications (word processing, photo editing)
- Individual applications

Data:

- Documents
- Photos
- Music, videos
- Email
- Class projects



Values of Assets





Beyond “Computer” Security

Mobile
Devices



IoT



Industrial
CPS (Cyber-
physical
system)



Stuxnet

- Stuxnet Worm Attack on Iranian Nuclear Facilities



Think like an attacker



If you know the enemy and know yourself you
need not fear the results of a hundred battles.

(Sun Tzu)

izquotes.com

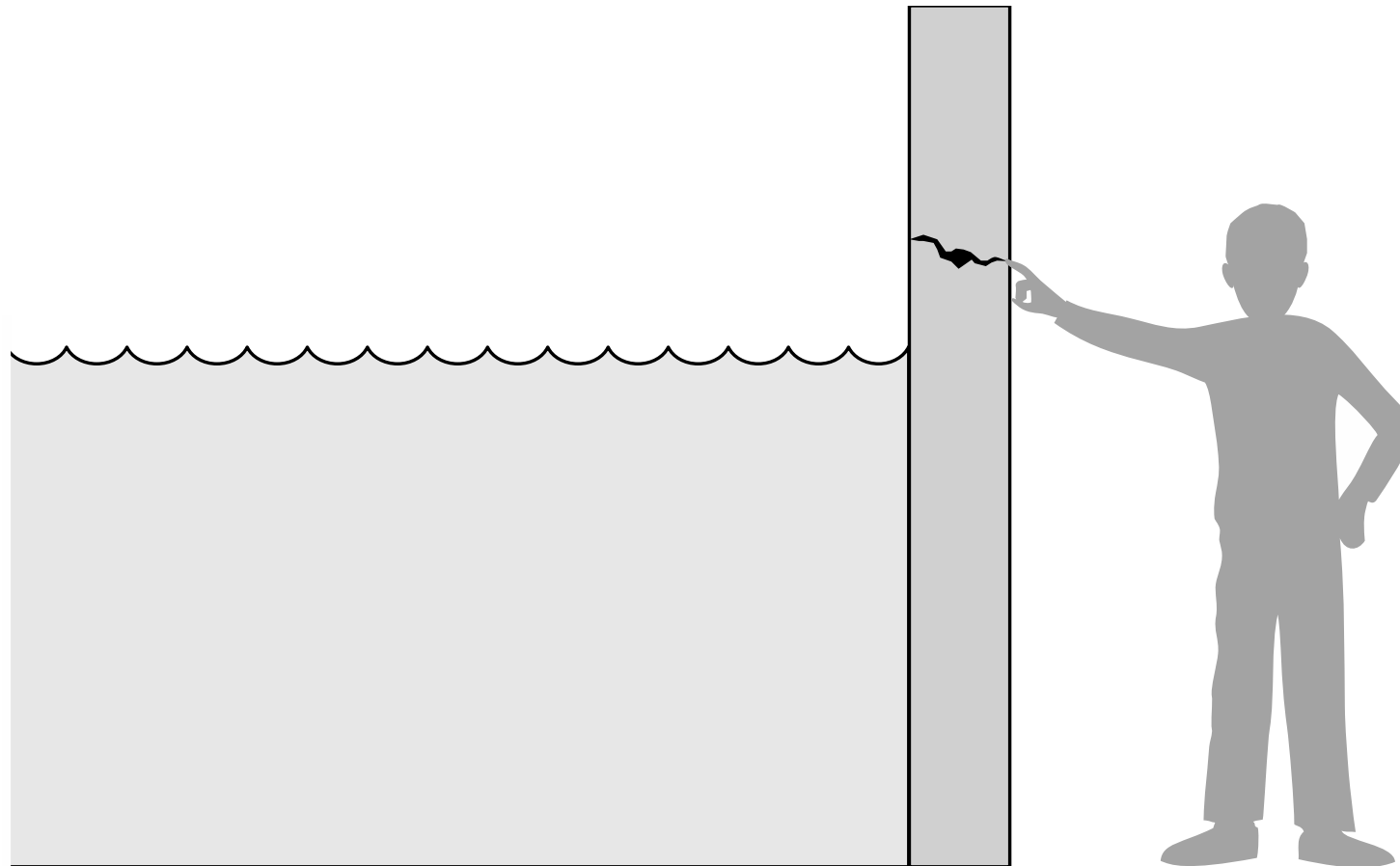


Vulnerability–Threat–Control Paradigm

- **Vulnerability**
 - “A vulnerability is a weakness that could be exploited to cause harm.”
- **Threat**
 - “A threat is a set of circumstances that could cause harm.”
- **Control**
 - “Controls prevent threats from exercising vulnerabilities.”



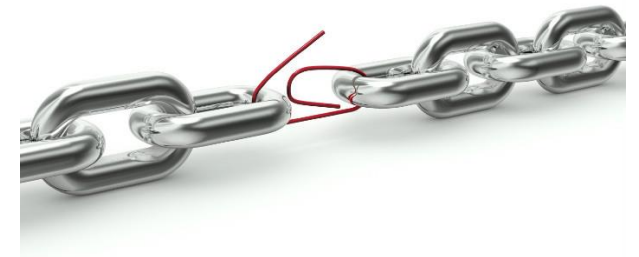
Threat, vulnerability and control





Think like an attacker

- Attacker, a.k.a., **adversary**
 - “A human who exploits a vulnerability perpetrates an attack on the system.”
- Attacker looks for weakest links – easiest to attack.
- **Threat/adversary model**
 - Assumptions of attacker’s capabilities
- Identify assumptions that security depends on.
 - Are they false? Can I make them false?
- Reduce **attack surface**.
 - “System’s full set of vulnerabilities—actual and potential”





Security properties (C-I-A triad)

- Confidentiality
 - Things you don't want others to know
- Integrity
 - Things you don't want others to change
- Availability
 - Things you want to ensure that can be used by legitimate parties
- Two other desirable characteristics (ISO 7498-2)
 - Authentication
 - Nonrepudiation



Question

- Can you give some examples about **breaking** security properties?
 - Confidentiality
 - Integrity
 - Availability