ENEE 457: Computer Systems Security 8/27/18

Lecture 1
Introduction to Computer Systems Security

Charalampos (Babis) Papamanthou

Department of Electrical and Computer Engineering
University of Maryland, College Park

Outline

- Definition of Computer Systems Security
- Common threats and defenses facing computer systems today
- Class logistics
- Some attacks that have taken place in the real world

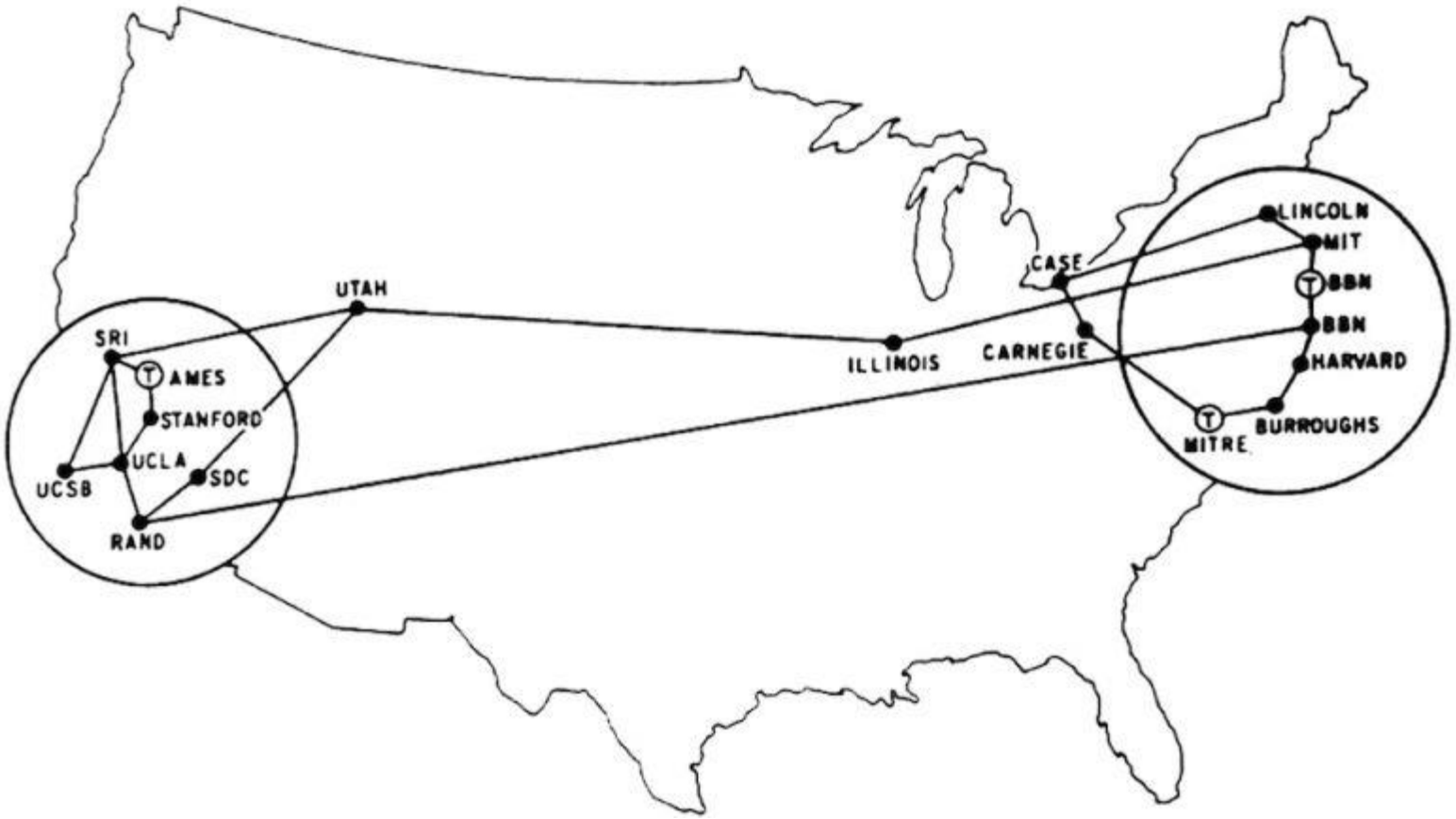
What is Computer Systems Security?

write software that is not only functional but…

…works even when malicious players interact with it …

What does this mean?

- In the beginning…

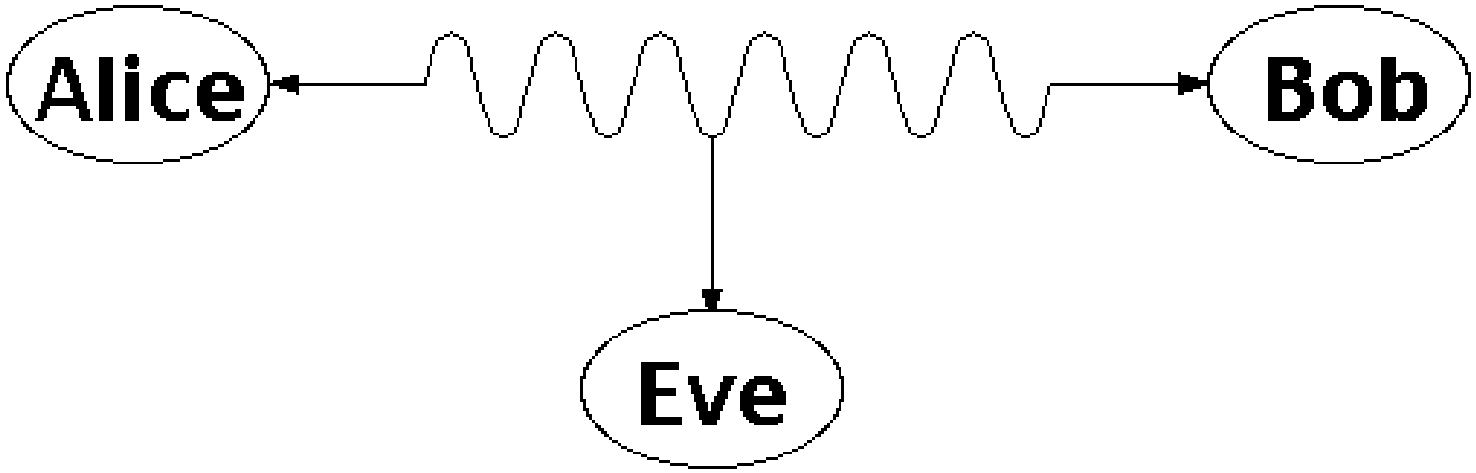


What does this mean?

- Now?

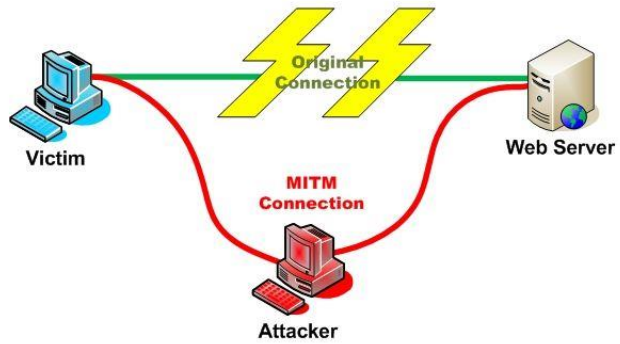
Threat #1: Eavesdropping of information

- The interception of information intended for someone else during its transmission over a communication channel
  - DEFENSE?
  - https://sela.io/pgp/
  - https://keybase.io/cpap/key.asc



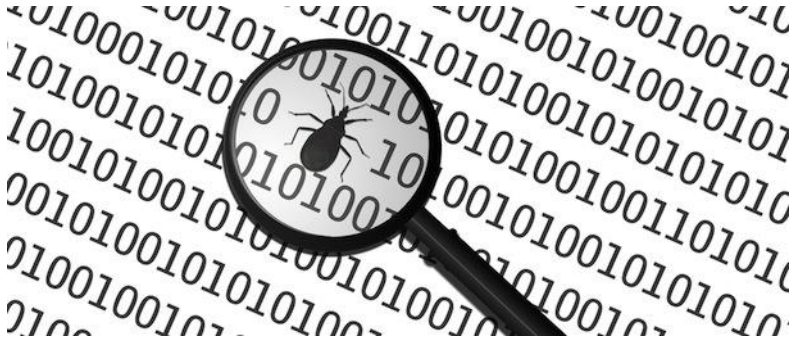
Threat #2: Alteration of information

- Unauthorized modification of information
  - Example: the man-in-the-middle attack, where a network stream is intercepted, modified, and retransmitted
  - DEFENSE?



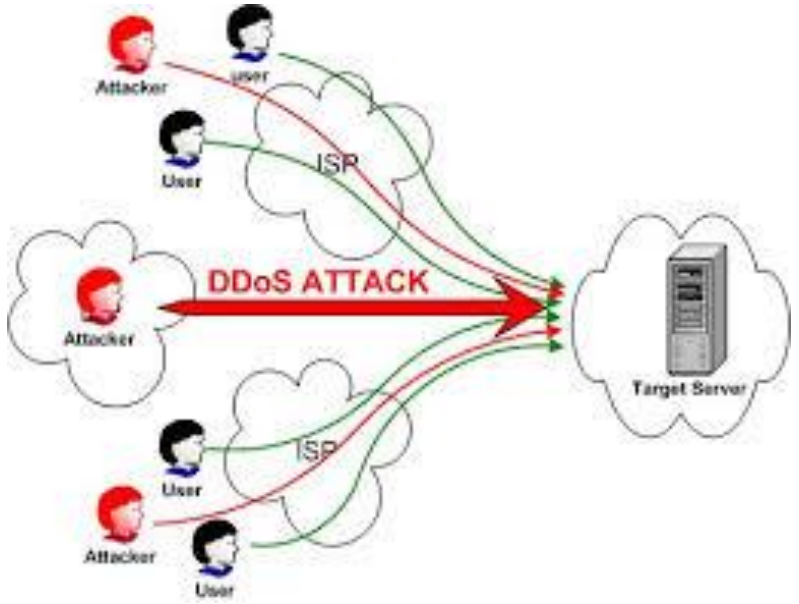
Threat #3: Software bugs

- Code has some bugs that do no affect functionality but can be exploited by an attacker
  - Example: Some application code is mistakenly using an algorithm for encryption that has been broken
  - Example: There is no checking of array bounds
  - DEFENSE?



Threat # 4: Denial of service

- The interruption or degradation of a data service or information access
  - Example: email spam, to the degree that it is meant to simply fill up a mail queue and slow down an email server
  - DEFENSE?



Threat # 5: Breaking passwords

- Defenses?

Threat #6: Sensitive data in the cloud

- Storing files in the cloud. Cloud gets to access data. How do we make sure cloud does not get to see data (e.g., Gmail)?
  - DEFENSE?
- We have 1,000 files and we encrypt them and then we store them in the cloud. While not the cloud cannot see the content, it can see the access patterns. How do we prevent that?
  - E.g., Imagive we run the program: If secret = 1 access A[5], else access A[19];
- Case study: Use a new protocol to access files (known as oblivious RAM). Read here

Organization

- Class webpage
  - http://enee457.github.io
  - Two lectures per week, MW 11am – 12.15 pm
- Professor
  - Charalampos (Babis) Papamanthou (cpap@umd.edu)
  - Office hours: Mon 12:30pm-2pm, AVW 3409
  - www.ece.umd.edu/~cpap
- TAs
  - Xinyu Zhou (xyzhou@terpmail.umd.edu) and Shravan Srinivasan (sshravan@cs.umd.edu)
  - Office hours: TBD
  - VERY IMPORTANT: GO TO THE TA SYSTEMATICALLY

Grading

- Final grade
  - 5 homeworks (20%)
  - 5 programming assignments (30%)
  - 1 Build-it-Break-It project (10%)
  - Midterm (10%): Wed Oct 17 in class
  - Final (25%): Fri Dec 16 in class (from 8am to 10am)
  - In class presentation of security vulnerabilities (5%) --- we need 10 groups
  - Extra credit (research project) (up to 10%): Implement E2E plugin for Gmail. Pls email Tas.
- Lectures will be published on the webpage after class
- Homeworks and programming assignments will be published on the class webpage, but should be submitted through Canvas
- No late homework submissions will be accepted
- Discussions will be managed at Canvas

Grading

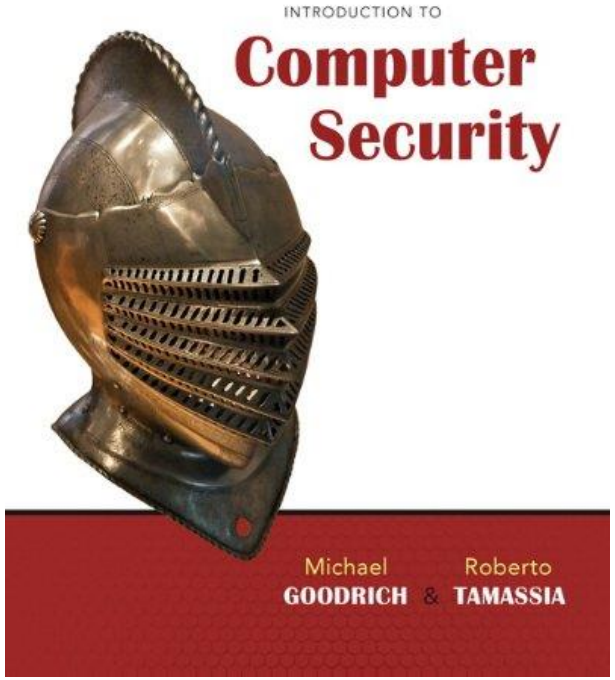
- Final grade
  - >90% A-,A,A+
  - >80% B-,B,B+
  - >70% C-,C,C+
  - >60% D-,D,D+
- Do not assume that there will be a curve

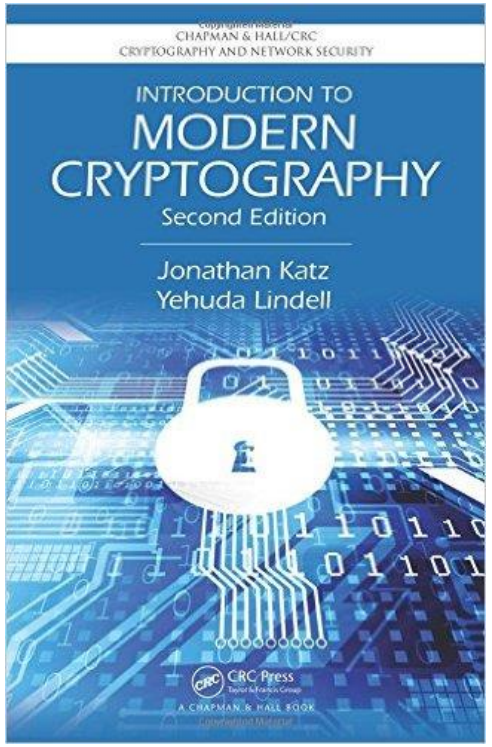
Prerequisites, CS classes and programming

- ENEE150 or CMSC132
- IMPORTANT: If you have taken CMSC414 in the past, I STRONGLY RECOMMEND AGAINST TAKING THIS CLASS
- MORE IMPORTANT: If you are currently taking CMSC414, please drop one of either CMSC414 or ENEE457
- The course will have a significant programming component
- Sample programming projects (FUN, FUN, FUN):
  - Writing code to break an encryption algorithm that I am going to give you
  - Writing code to log into a server (without credentials) which will be running a buggy version of Linux
  - Inspecting buggy code that I will give you and try to exploit its vulnerabilities
  - Writing code to crack passwords
- Knowledge of algorithms and data structures is desirable

Readings

- Most of the class will be based on the following textbooks (GT) and (KL):





- We are going to be using the board too, so it is advisable you keep notes as well
- The library has copies of the book

Other readings

- Other recommended readings are (WS) and (KPC)