CS 493 - Computer Security

Note Title 1/14/2011

Today

- Syllabus
- Ethics!
- Definitions & Intro

This course:

- Homework
- Lab attendance + occasional pop quizzes
- Paper reviews
- Lab assignments
- Midterm + final exam

Look for syllabus next time.

Some things to note:

- Late policy for assignments.

- Paper reviews: You will write in this course!

- Labs - on a remote system called DETER

- Course resources - the internet is fair game, but cite your sources! (& use common sense)

Workload

This is a senior level topics course!
I will expect a lot of reading & independent work.

Ethics and Computer Security

1. "Hacking" is not glamorous

(pause for movie clips)

② Indiscretions now can (& probably will) haunt you later

So: Before you experiment, I suggest talking to me!

This course walks a fine line, & playing will get you into trouble.

Course policy

Any malicious behavior (as I define it) will result in an immediate F, an official complaint on your student record, & forwarding of the details to the dean.

In addition, I will report you to legal authorities.

What is Security?

(Hint: The word "computer" should not be in your answer.)

Access control

physical safety/control

Why security?

- Money
- Safety
- Reputation

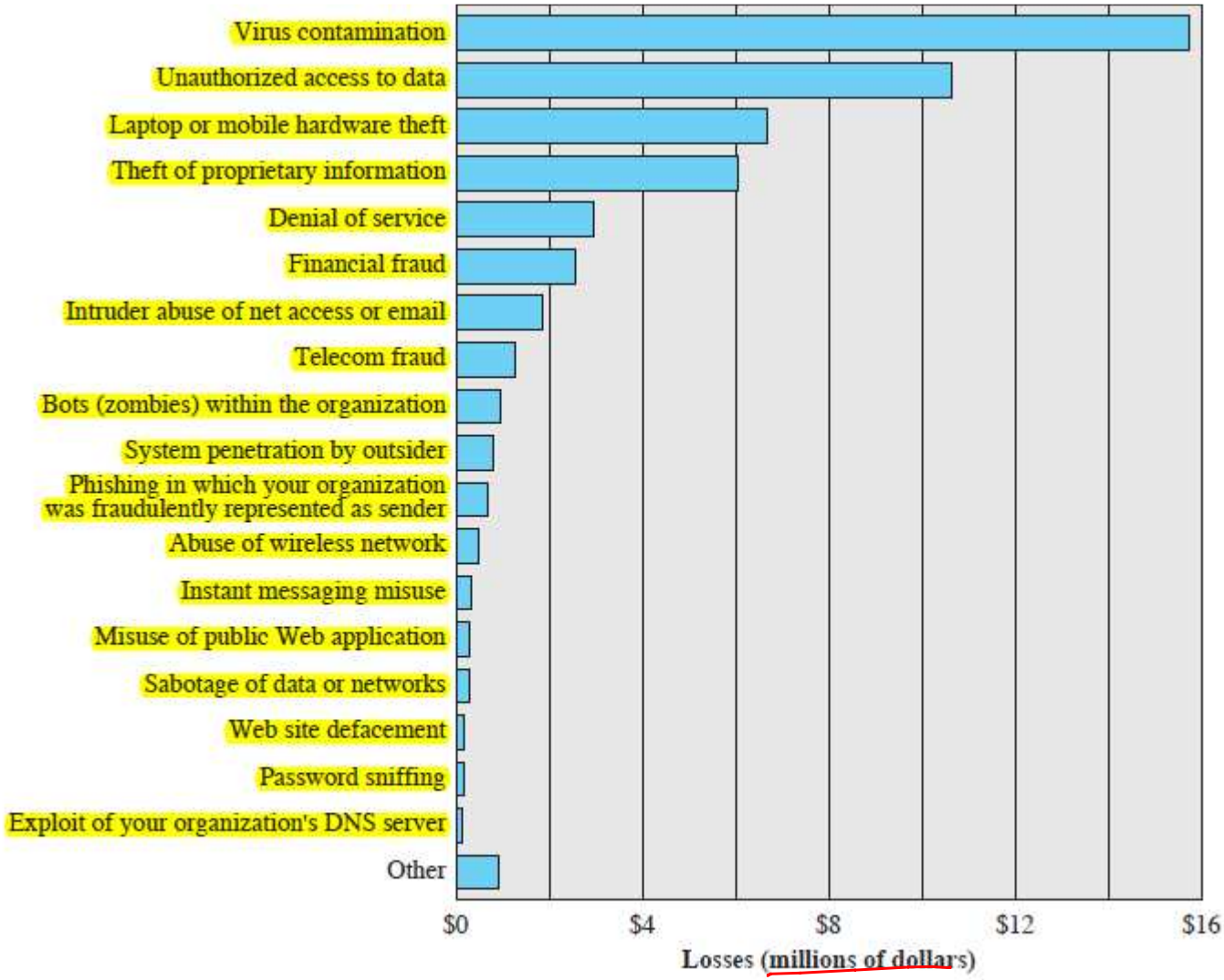


Image provided by William Stallings and Lawrie Brown, with permission.

Security did not begin with computers.

8500 BC: Farmers store food in a communal warehouse.

Clay tokens represented food stores.

How to avoid cheating?

MS 4631
Bulla-envelope with 11 plain and complex tokens inside.
Near East, ca. 3700-3200 BC

Solution: Tokens are placed in clay envelope, sealed at warehouse.

When a farmer wants his food, it is broken in front of a witness.

(This is the origin of today's coin.)

12th Century: Jewish book keepers want a way to ensure integrity in their books!

Solution: Double-entry bookkeeping.

Account paid

Account receiving

(Still used today in banks.)

19th Century: The heliograph is used to signal Morse code

Image provided by Wikimedia Commons.

From 1834-1836, two bankers bribed an operator to provide information about the stock market by making mistakes in the transmission.

(Now called a covert channel attack.)

Basic Issues :

1) Confidentiality

2) Integrity

3) Availability

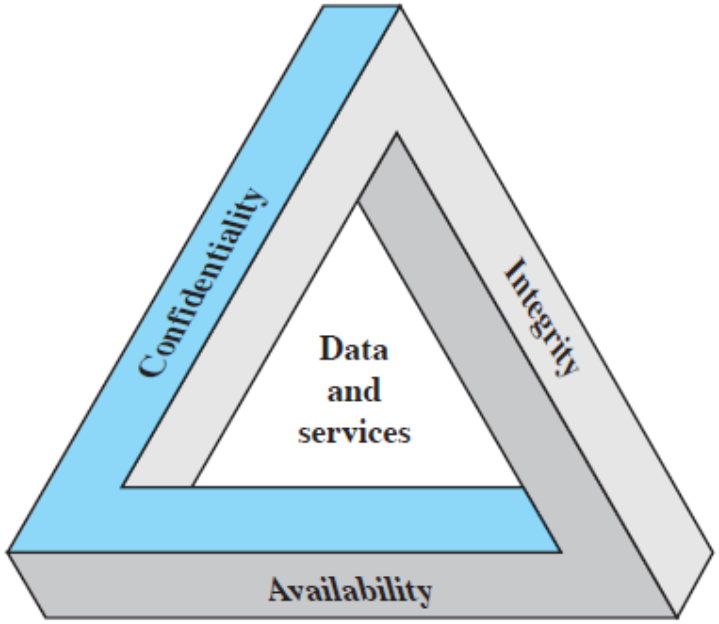


Figure 1.1 The Security Requirements Triad

Image provided by William Stallings and Lawrie Brown, with permission.

Confidentiality:

- data confidentiality
- privacy

Example: Student grade information.

Grades are confidential. (high confidentiality)

Class roster. - medium

Phone number.

Integrity:

- data integrity
- system integrity

Example: Doctor's records

Accurate records

Accessibility

No unauthorized Changes

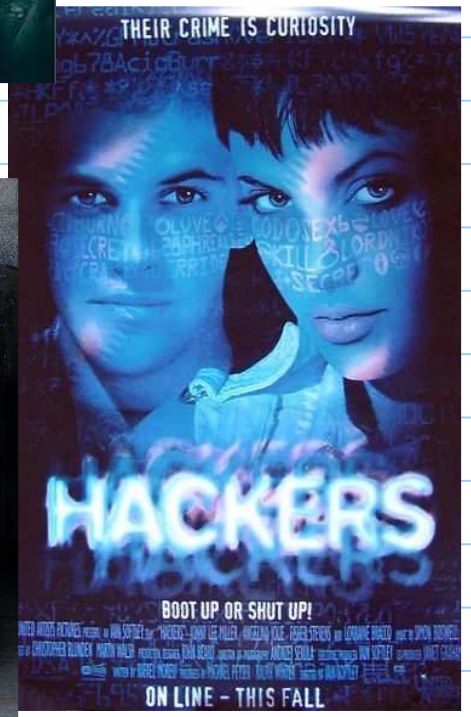
Availability:

- system should be available to users

Examples: Web sites

- Your homework (low)
- Bank account (medium)
- 911 call center
- DNS server

Sounds pretty boring



It's fiction, people!

In reality, it's mostly:

- resetting passwords
- attempting to convince people that they really do need to be careful
- advanced mathematics