CS443 - Computer Security

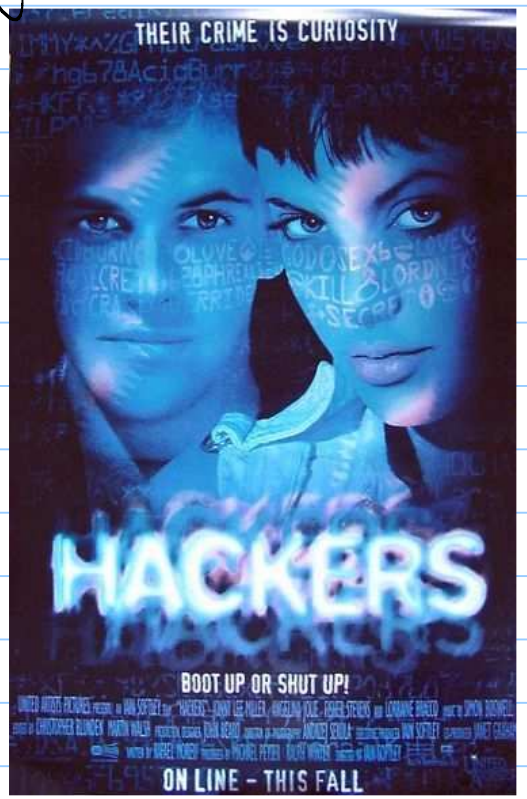
Note Title 1/14/2013

Today:

- Syllabus
- Lab overview + lab 1
- Intro to security
- A note on ethics

Computer Security: Public perception

- glamorous & dangerous
- exciting



Reality: Often very boring.

- Detailed & difficult coding.
- High level mathematics.
- Changing permissions & lecturing users about their passwords.

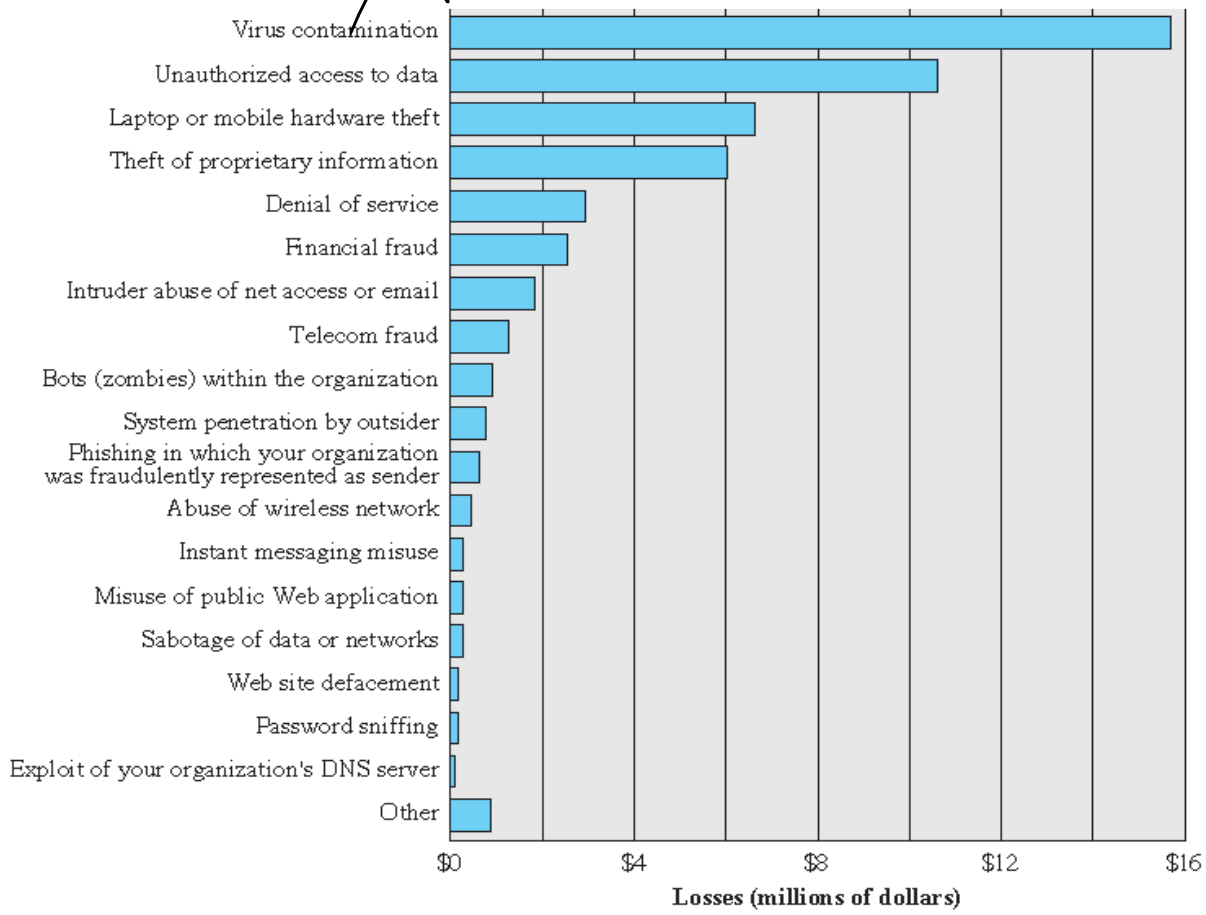
My Goal:

Introduce both theory and practice of computer security.

- You will be asked to attack and harden machines & software.
- You will also be required to write essays based on research articles. Emphasis will be on clear communication of issues & your opinion.

(This part is generally more difficult!)

Why Security?



(from an FBI survey)

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

Security issues certainly predate computers

8500 BC: Food is stored in communal warehouse.

Tokens are placed in a clay envelope & sealed by warehouse.

Envelope broken in front of witnesses when farmer wants his share back.

(This evolved into coins later.)

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

12th century: Jewish bookkeepers invent double entry bookkeeping to maintain 'integrity'.

Each transaction recorded in 2 separate books.

This technique is still used in modern banking.

Draper's Shop. Woodcut by Erhard Schoen. 1518.
Image provided by ARTStor.

Assurance issues:

The heliograph was used in the 19th century to transmit Morse code.

Image provided by Wikimedia Commons.

In the 1830's, two French bankers bribed an operator to make mistakes in transmissions to signal information about the stock market.

(Today, we call this a covert channel attack.)

Basic Issues:

- How do you know who you are speaking to?
- How do you verify accuracy & honesty?
- How do you know when & where goods will arrive, & if valid payments will be provided?

The C.I.A. Triad

3 essential components:

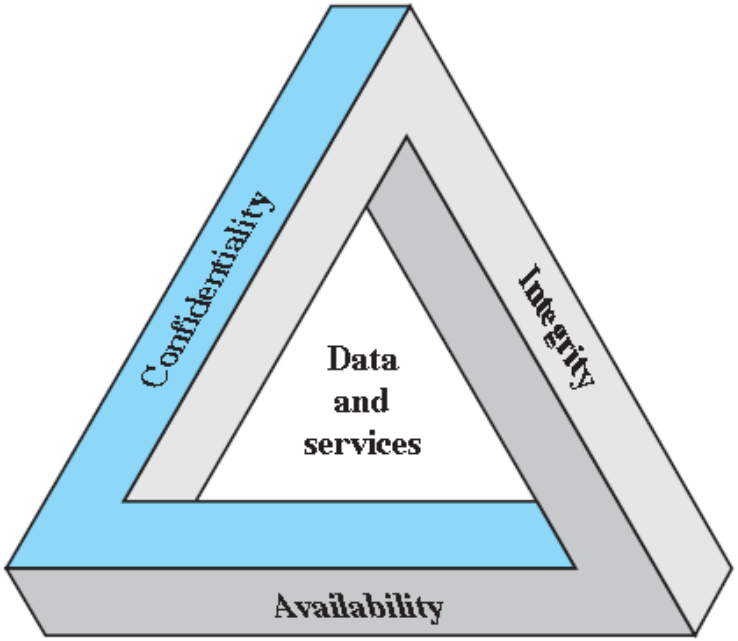


Figure 1.1 The Security Requirements Triad

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

Confidentiality: concealment of resources

- data confidentiality
- privacy

Ex: How does confidentiality apply in a college?

Integrity : trustworthiness of resources

- data integrity
- system integrity

Ex: Medical records system

Availability: access to resources

- Again, both systems + data should be available.

Generally, this requirement is in direct conflict with the previous two.

The more available (+ usable) systems are also often less secure (and more expensive).

Ethical behavior

In this class you will learn things you can use to break the law.

In particular, labs are set up to give hands-on practice in a safe setting.

Conduct yourself with integrity.
(And remember - I am neither your mother nor your babysitter.)

Essay: "The Law of the Horse"
by Lawrence Lessig, professor of law
at Harvard, in 1999

There may not be
"cyberlaw" as a field,
conduct is still defined
in the CS field by:
- laws
- norms
- market
- architecture (or codes)

Laws: CFAA in 1986

Protects confidentiality of private information.

It is a crime to "knowingly access a computer without or in excess of authority to obtain classified information".

Also a crime to access any "protected computer" without authorization even if no damage is done.

Norms:

While not legally binding, social norms certainly drive our behavior effectively.

> "Norms regulate behavior in cyberspace as well: talk about democratic politics in the alt.knitting newsgroup and you open yourself up to 'flaming'...'Spoof another's identity in a 'MUD' and you may find yourself 'toaded.'"
>
> -- Lessig

Market: regulates price & services

Obviously, the cost of the internet is a factor.

But digital issues are more complex. In his essay, Lessig says:

> "Think of it like this: Today when you buy a book you have the 'right' to do any number of things with that book."

He goes on to muse how different pricing might be if the seller could regulate sharing, copying, or even # of times to read the work.

Eerie Coincidence:

In 2008, Amazon added several Orwell books to the kindle store.
They did not have rights to them.

Amazon deleted the works from buyer's library.

However, this deleted their own work (such as annotations) also.

Code:

The internet is built on codes.

- TCP / IP
- Crypo protocols
- server / router infrastructure

These seriously constrain behavior.

Next time:

An overview of cryto + hashing.