Introduction to Computer Security

Coverage in Midterm: 5%

Bo Luo
bluo@ku.edu

Concepts,principles,etc.
– Principle of Easiest Penetration
• Identify easiest penetration in real world scenarios
– Threats, vulnerabilities, controls
– Kinds of threats: interception, interruption, modification, fabrication
– MOM: method, opportunity, motive
– Meaning of computer security: CIA – confidentiality, integrity, availability
– Hardware, software, and data
– Defense: prevent, deter, deflect, detect, recover
– Principle of Effectiveness, Principle of Weakest link

Course objectives

- Understand the basic principles and problems of computer security
  - understand the basic concepts & principles
  - examine *security risks*
  - consider *countermeasures* or *controls*
  - think about uncovered *vulnerabilities*
  - identify areas where more work is needed

What's Valuable?

- Important to protect what's valuable
- Bank example:
  - Protect money well
  - Forget to protect the customer information
  - Now: Regulations for Financial Institutions and Customer Information

Principle of Easiest Penetration

- Intruder will use *any* means of penetration.
- Site or method of penetration
  - May not be most obvious
- Not necessarily where the strongest defenses are
  - e.g., don't install strong lock but not hinge
  - Yes, intruders are (always) able to find the easiest penetration!

Valuable Components

- Computer's "valuable components"
  - hardware
  - software
  - data
- Any can be targeted

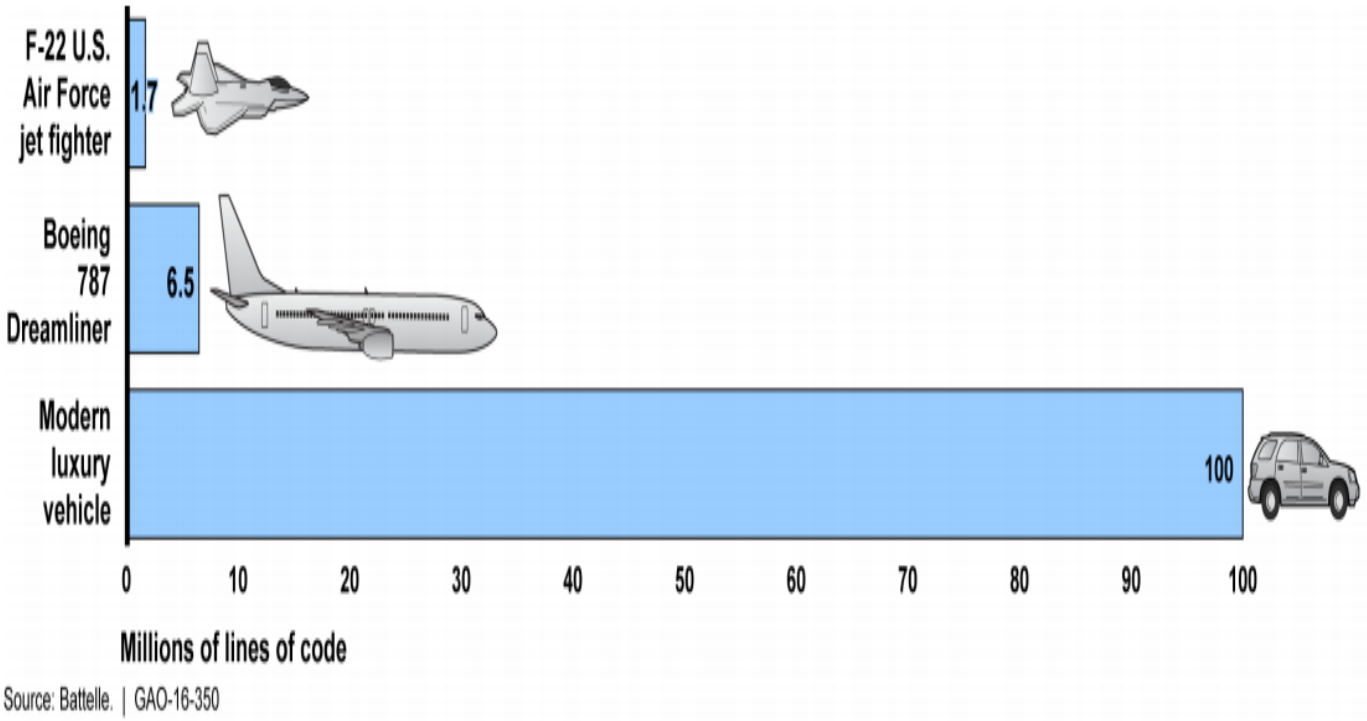
- Could be mixed
  - Attacking from hardware, targeting at data

Automobile Example

- Modern cars have many computer systems
- Do they need security?

Automobile Example

- Modern cars have many computer systems
  - Bug to code ratio: 15 and 50 bugs per 1,000 lines of code
  - Hoe many lines of code in your car?



Automobile Example

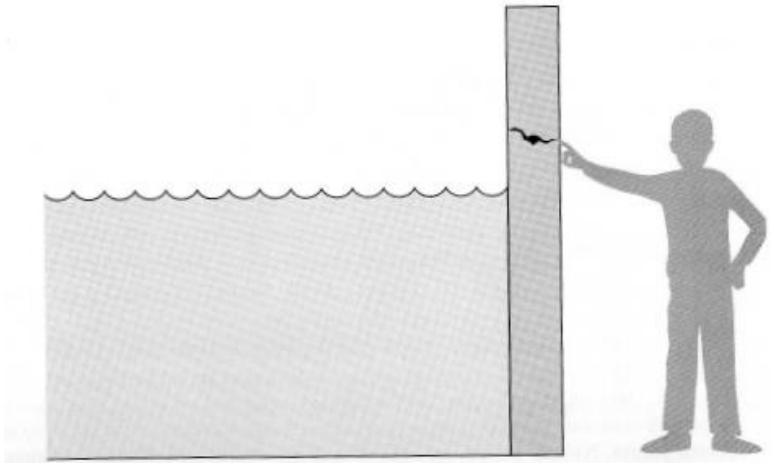
- Modern cars have many computer systems
- Do they need security?
- False assumptions:
  - the code is too complex for troublemakers
    - the more complex, the more difficult to make secure
  - why would anyone want to hack them?
    - disable alarms, unlock doors, tracking
    - just because they can

Software Security

- Modern cars have many computer systems
- Do they need security?
- Attack example:
  - Tire Pressure Monitoring System (TPMS) signal sent wirelessly
  - Easily eavesdropped, with unique identifier
  - Easily spoofed, to trigger alert messages

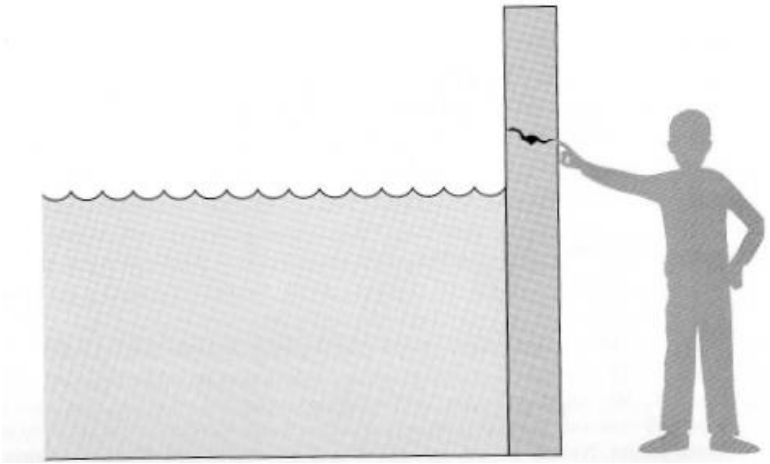
Threat vs. Vulnerability

- *Vulnerability*: security weakness that might be exploited to cause undesired consequences
- *Threat*: a set of circumstances that potentially cause loss or harm.
- *Attack*: the exploitation of vulnerabilities by threats.



Threat vs. Vulnerability

- Water is the *threat*
- Crack is *vulnerability*
- Threats can be:
  - human initiated
  - computer initiated
- Threats can be:
  - attacks
  - mistake
  - failure



Controls

- A *control* is a protective measure
- A *threat* is blocked by a *control* of a *vulnerability*

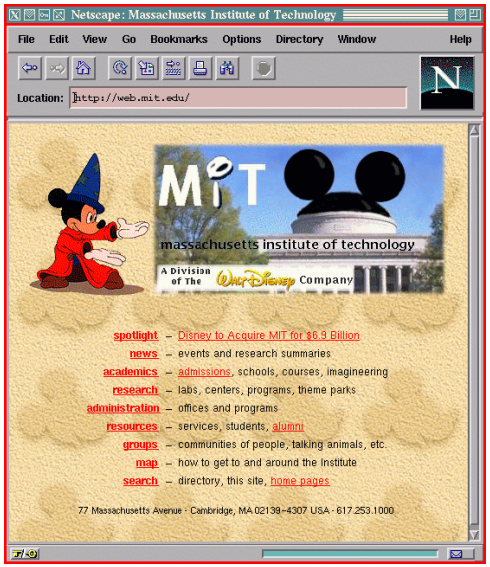
Types of Threats

- Interception
- Interruption
- Modification
- Fabrication

MOM

- For a successful attack, attacker must have:
  - Method: skills, knowledge, tools to pull off the attack
  - Opportunity: time and access
  - Motive
- Control?
  - Eliminate one of them…

Universities Are (Still?) Prime Targets



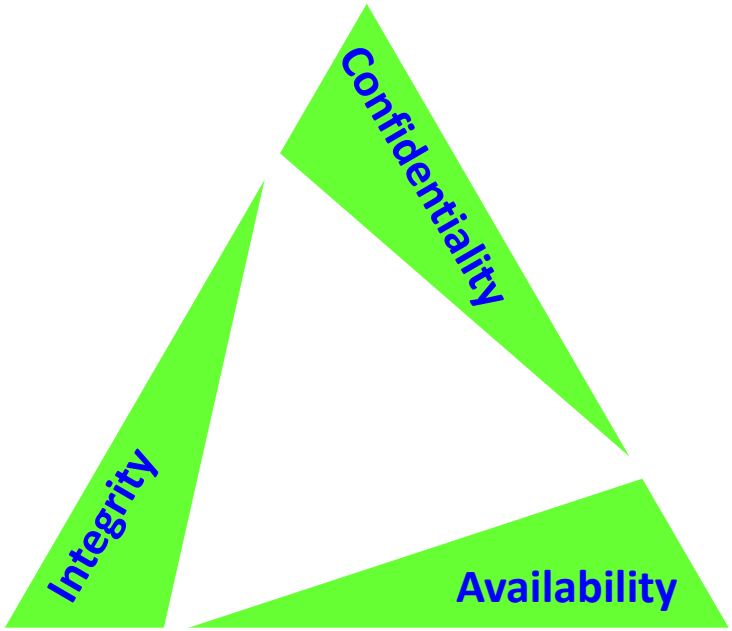
Universities Are (Still?) Prime Targets

- Universities often:
  - run systems with vulnerabilities
  - have little monitoring
  - have little management
- Universities promote free exchange of ideas
  - wide access
- Student population frequently changes
  - old accounts stay around
  - often student workers (little training)
- Many departments
  - one dept. doesn't always know what the other is doing

Meaning of Computer Security

- Security should provide:
  - confidentiality
  - integrity
  - availability (implies *timely availability*)

- The CIA notion
- Other factors?
  - Authentication
  - Authorization
  - Non-Repudiation
  - Privacy



Vulnerabilities

- Consider three types:
  - hardware
  - software
  - data

Hardware Vulnerabilities

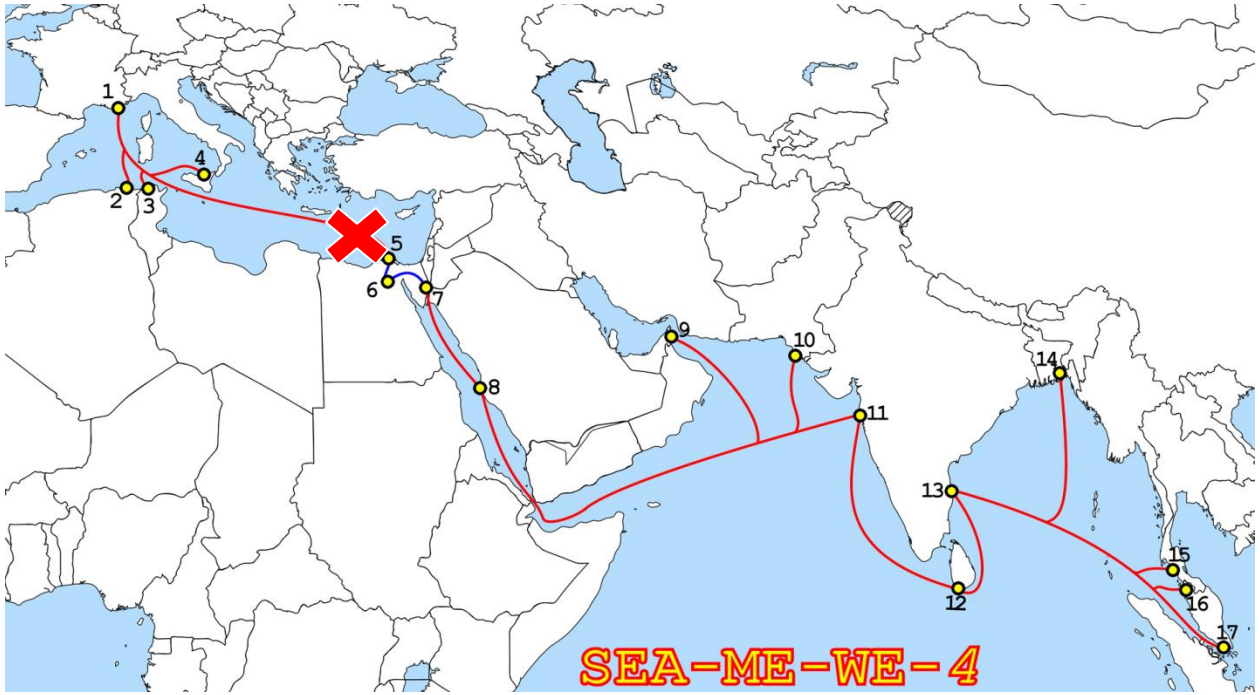
- Often easiest to defend against
- Examples:
  - adding/removing/changing devices
  - pull the plug
  - spill soda
  - reboot with boot disk to use machine for attack,
  - mount HDs, etc.

"Backhoe" vulnerability?

- When company digs, registers with locality
  - utilities in dig zone spray paint what's buried
  - item not marked, or digger doesn't contact locality?
- Backhoe cutting fiberoptic cable
  - most common cause of telecom outages
- Publicly available information
- Single cuts can cause widespread outages
- Telecoms reluctant to lay redundant cable
- Legitimate threat?

Forget hoes. what about anchors?

- 2/2008. Two undersea cuts to SeaMeWe4
  - South East Asia–Middle East–Western Europe 4
  - Optical fiber submarine communications cable



Forget hoes. what about anchors?

- 2/2008. Two undersea cuts to SeaMeWe4
  - South East Asia–Middle East–Western Europe 4
  - Optical fiber submarine communications cable
- Major disruptions in Middle East, S. Asia
  - Egypt 70% lost capacity
- Both cuts just off coast of Alexandria
  - Redundant cable.
  - Geographic diversity?

Personal hardware?

- Implanted medical devices, e.g.
  - vulnerable defibrillator with wireless access
- BYOD
  - Connect your own phone/laptop to the corporate WiFi?
  - Receive emails on your personal tablet?

CPU?

- Meltdown & Spectre
  - Out-of-order execution & speculative execution
  - Caching

Software Vulnerabilities

- Breaking software
- Modify to do something different
  - e.g. bank software **salami attack**, or send duplicate of all transactions to attacker
- Delete software
- Software theft
- Can use configuration management to avoid software modification attacks.
- Need a root of trust…

Vulnerability Window

- Vulnerability "life cycle"
  - Born (in software, hardware)
  - Discovered, not yet patched (0-day)
    - May be known to the public
  - Patched
- Most vulnerable before they are patched

- 0-days are valuable
  - Black market
  - Software vendors give rewards

Data Vulnerabilities

- Data can be understood by lay people
  - e.g. SSN, address, name …
  - don't need:
    - physical access (as in HW vulnerabilities)
    - computer skills (as in SW vulnerabilities)
- Can be very valuable
  - e.g. private company info.
- Can be damaging if modified
  - e.g. air traffic control, patient drug allergies

How Long Are Data Valuable?

- Might only be valuable for short time
  - *e.g.* Oscar winners, movie *Trading Places*
- Principle of Adequate Protection
  - Items must be protected only until they lose value
  - Must be protected to degree consistent with value

Data Confidentiality

- Data can be compromised by:
  - wiretaps
  - bugs in output devices
  - bugs in input devices, *e.g.*, keystroke loggers
  - monitoring electromagnetic radiation
  - inferring one data point from other
  - just asking

Data Integrity

- Concerned about data modification
- Change often more effort than reading
- Some sophisticated examples:
  - salami attacks
  - replay

Risk Assessment

- ISO 27005 framework
  - Risk analysis
    - Risk identification
    - Risk estimation
  - Risk evaluation

Top Methods for Attack

- Information Week Survey (2001)
  - survey of security professionals
- Attacks:
  - 33% OS vulnerabilities
  - 27% unknown application vulnerabilities
  - 22% passwords
  - 17% abuse of valid accounts & permissions
  - 12% internal denial of service
- Note - 80% done by insiders

The Insider Problem

- Most defense mechanisms are designed for external attacks
- Makes it more vulnerable to insider attacks
  - Firewalls: crunchy on the outside, soft and chewy on the inside
- Policies and policy enforcement

- How about outsiders with knowledge from insiders?
- Trojan horses?

Attack Timing

- Consistently scanning the network
- Triggered by an event
- Triggered by the user
- Controlled by the attacker

Adversaries – Computer Criminals

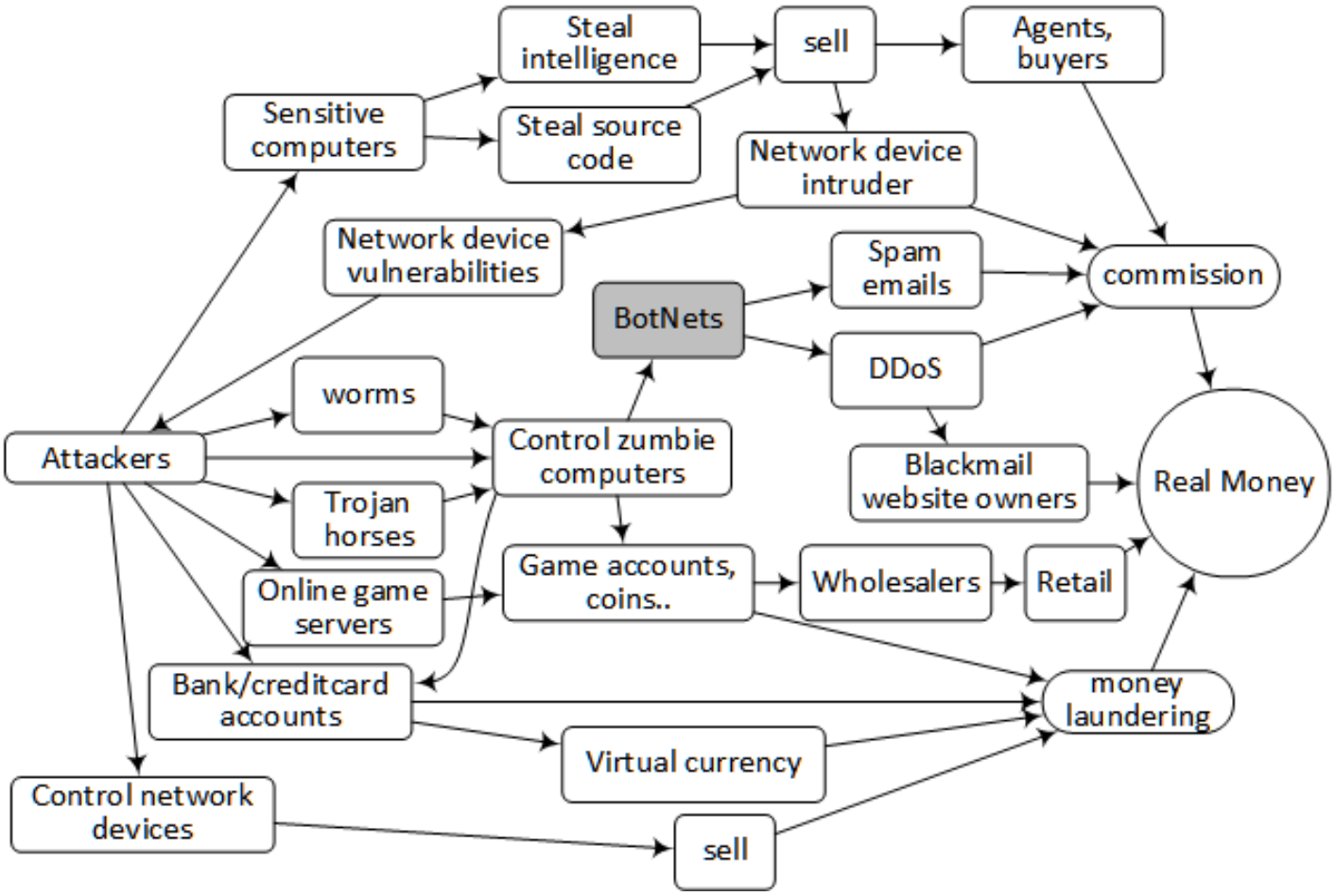
- Script kiddies
  - download tools
  - don't understand them
- Amateurs
  - Average user who stumbles upon vulnerability
- Crackers
  - Hack for the challenge
- Career criminals
  - hack for personal profit
- Users with skills
  - design, implement tools

Market for Stolen Data

- Black/gray market
  - Bank accounts
  - Credit card numbers
  - SSN
  - User information

  - Accounts, passwords, etc.

FYI: the economy of computer crime



Methods of Defense

- **Prevent -** close vulnerability
- **Deter -** make attack more difficult
- **Deflect -** make another target attractive
- **Detect -** know when attack occurs
- **Recover -** mitigate attack's effects

Controls in Computer Security

- Encryption
- Software controls
- Hardware controls
- Policies and procedures
- Physical controls

Controls: Encryption

- Important part of security
- But many more things in the picture
  - Bellovin survey of CERT vulnerabilities
- Much more about encryption later

Controls: Software

- Internal program controls
  - part of program
  - enforces security restrictions
    - *e.g.*, access ctrl in DBMS
- OS, network controls
  - same for OS, nets
  - protect OS, net from users
  - protect users from each other

Controls: Software

- Independent control programs
- – *e.g.*, password checkers, IDS, antivirus
- Development controls
  - quality standards
  - used during:
    - design
    - coding
    - testing
    - maintenance

Controls: Hardware

- Examples
  - smart cards
  - locks, cables
  - user identification devices
  - firewalls
  - IDS
  - circuit boards that control access to storage media

Controls: Policies & Procedures

- *i.e.*, *"human"* policies and procedures
- Very important, often overlooked
- Examples:
  - Proper use of passwords (password policies)
  - What not to write in email
  - What not to say over the phone
  - What not to say to strangers (or let overheard)
    - Probes for stock insider info, HIPAA, etc.
  - Documents to shred or not

Controls: Physical

- Examples:
  - guards
  - locks
  - backups (including off site)
  - *etc*.

The Security Lifecycle

Defense in Depth

- What if the control mechanism fail?
- Defense in Depth (Castle Approach)
  - Originated from a military concept
  - Layered control mechanisms
  - Distributed defense
  - Redundancy in defense
  - For all aspects: physical, hardware, software, policies, personnel, etc.
  - Example: anti-spam

Principle of Effectiveness

- Controls must be used and used properly to be effective
- They must be:
  - efficient
  - easy to use
  - appropriate

Principle of Weakest Link

- Security is no stronger than the weakest link
- Weakest link can be:
  - Firewall's power supply
  - OS that a security app runs over
  - Human who:
    - plans
    - implements or
    - administers controls