CENG 374E - INTRODUCTION TO COMPUTER SECURITY

Prof. Dr. Şeref SAĞIROĞLU

Gazi University
Engineering Faculty
Computer Engineering Department
Maltepe/Ankara

SS@gazi.edu.tr
https://avesis.gazi.edu.tr/ss

Computer Security in Practices

Information hiding

Security

Applications

Negotiation

Privacy

Integrity

Access control

Threats

DATA PROVENANCE

Biometrics

Semantic web security

Fraud

TRUST

POLICY MAKING

Encryption

Computer epidemic

Data mining

Anonymity

Formal models

System monitoring

Vulnerabilities

Network security

Statistics

- 40% detected **external penetration**

- 40% detected **denial of service attacks**.

- 78% detected employee **abuse of Internet access privileges**

- 85% percent detected **computer viruses**.

- 38% suffered **unauthorized access** or misuse on their Web sites within the last twelve months.

- 12% reported theft of transaction information.

- 6% percent reported financial fraud.

Critical Infrastructure Areas

include:

- Telecommunications
- Electrical power systems
- Water supply systems
- Gas and oil pipelines
- Transportation
- Government services
- Emergency services
- Banking and finance
- ...

What is a "Secure" Computer System?

- To decide whether a computer system is "secure", you must first decide what "secure" *means to you*, then identify the threats you care about.

You Will Never Own a Perfectly Secure System!

What is a "Secure" Computer System?

- Threats - examples
  - Viruses, trojan horses, etc.
  - Denial of Service
  - Stolen Customer Data
  - Modified Databases
  - Identity Theft and other threats to personal privacy
  - Equipment Theft
  - Espionage in cyberspace
  - Hacktivism
  - Cyberterrorism
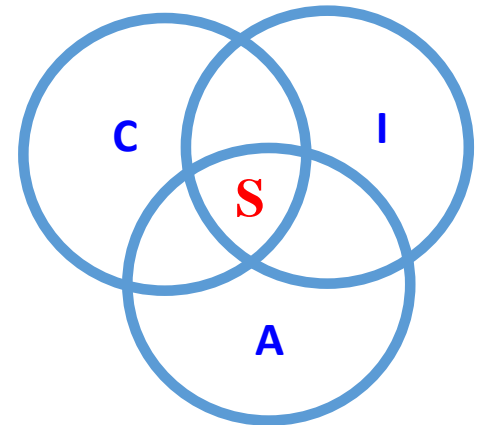 - …

Basic Components of Security:
Confidentiality, Integrity, Availability (CIA)

- CIA
  - Confidentiality: Who is authorized to use data?
  - Integrity: Is data …. good?"
  - Availability: Can access data whenever need it?

- CIA or CIAAAN… ☺

  (other security components added to CIA)
  - Authentication
  - Authorization
  - Non-repudiation
  - …

S = Secure

Need to Balance CIA

- Example 1: C vs. I+A

  - Disconnect computer from Internet to increase confidentiality

  - Availability suffers, integrity suffers due to lost updates

- Example 2: I vs. C+A

  - Have extensive data checks by different people/systems to increase integrity

  - Confidentiality suffers as more people see data, availability suffers due to locks on data under verification)

Confidentiality

- "Need to know" basis for data access
  - How do we know who needs what data?
    Approach: access control specifies *who* can access *what*

  - How do we know a user is the person she claims to be?
    Need her identity and need to verify this identity
    Approach: identification and authentication

- Analogously: "Need to access/use" basis for physical assets
  - E.g., access to a computer room, use of a desktop

- Confidentiality is:
  - difficult to ensure
  - easiest to assess in terms of success (binary in nature: Yes / No)

Integrity

- Integrity vs. Confidentiality
  - Concerned with unauthorized *modification* of assets (= resources)
    Confidentiality - concered with *access* to assets

  - Integrity is more difficult to *measure* than confidentiality
    Not binary – degrees of integrity
    Context-dependent - means different things in different contexts
    Could mean *any subset of* these asset properties:
    { precision / accuracy / currency / consistency /
    meaningfulness / usefulness / ...}

- Types of integrity—an example
  - Quote from a politician
  - Preserve the quote (data integrity) but misattribute (origin integrity)

Availability

- Not understood very well yet

  Full implementation of availability is security's next challenge"

  E.g. Full implemenation of availability for Internet users (with ensuring security)

- Complex

  Context-dependent

  Could mean *any subset of* these asset (data or service) properties :

  { usefulness / sufficient capacity /

  progressing at a proper pace /

  completed in an acceptable period of time / ...}

Availability

- We can say that an asset (resource) is available if:

  - Timely request response
  - Fair allocation of resources (no starvation!)
  - Fault tolerant (no total breakdown)
  - Easy to use in the intended way
  - Provides controlled concurrency (concurrency control, deadlock control, …)

Vulnerabilities, Threats, and Controls

- Understanding Vulnerabilities, Threats, and Controls

  - Vulnerability = a weakness in a security system

  - Threat = circumstances that have a *potential* to cause harm

  - Controls = means and ways to block a threat, which tries to exploit one or more vulnerabilities
    - Most of the class discusses various controls and their effectiveness

- Example - New Orleans disaster (Hurricane Katrina)
  - Q: What were city vulnerabilities, threats, and controls?
  - A: Vulnerabilities: location below water level, geographical location in hurricane area, …
    Threats: hurricane, dam damage, terrorist attack, …
    Controls: dams and other civil infrastructures, emergency response
    plan, …

- Attack (materialization of a vulnerability/threat combination)
    - = exploitation of one or more vulnerabilities by a threat; tries to defeat controls
        - Attack may be:
            - *Successful*   (an *exploit*)
                - resulting in a breach of security, a system penetration, etc.
            - *Unsuccessful*
                - when controls block a threat trying to exploit a vulnerability

Threat Spectrum

- Local threats
  - Recreational hackers
  - Institutional hackers

- Shared threats
  - Organized crime
  - Industrial espionage
  - Terrorism

- National security threats
  - National intelligence
  - Info warriors

Kinds of Threats

- Kinds of threats:
  - Interception
    - an unauthorized party (human or not) gains access to an asset
  - Interruption
    - an asset becomes lost, unavailable, or unusable
  - Modification
    - an unauthorized party changes the state of an asset
  - Fabrication
    - an unauthorized party counterfeits an asset

- Examples?

Levels of Vulnerabilities / Threats

(reversed order to illustrate interdependencies)

- D) for other assets (resources)
  - including people using data, s/w, h/w

- C) for data
  - «on top» of s/w, since used by s/w

- B) for software
  - «on top» of h/w, since run on h/w

- A) for hardware

A) Hardware Level of Vulnerabilities / Threats

- Add / remove a h/w device
  - Ex: Snooping, wiretapping

    Snoop = to look around a place secretly in order to discover things about it or the people connected with it. [Cambridge Dictionary of American English]
  - Ex: Modification, alteration of a system
  - …

- Physical attacks on h/w   => need physical security: locks and guards
  - Accidental (dropped PC box) or voluntary (bombing a computer room)
  - Theft / destruction
    - Damage the machine (spilled coffe, mice, *real* bugs)
    - Steal the machine
    - „Machinicide:" Axe / hammer the machine
    - …

Example of Snooping:
Wardriving / Warwalking, Warchalking

- Wardriving/warwalking -- driving/walking around with a wireless-enabled notebook looking for unsecured wireless LANs

- Warchalking -- using chalk markings to show the presence and vulnerabilities of wireless networks nearby
  - E.g., a circled "W" -- indicates a WLAN protected by Wired Equivalent Privacy (WEP) encryption

B) Software Level of Vulnerabilities / Threats

- Software Deletion
  - Easy to delete needed software by mistake
  - To prevent this: use *configuration management software*

- Software Modification
  - Trojan Horses, , Viruses, Logic Bombs, Trapdoors, Information Leaks (via covert channels), …

- Software Theft
  - Unauthorized copying
    - via P2P, etc.

Types of Malicious Code

Bacterium - A specialized *form of virus* which does not attach to a specific file. Usage obscure.

Logic bomb - Malicious *[program] logic* that *activates when specified conditions are met.* Usually intended to cause denial of service or otherwise damage system resources.

Trapdoor - A hidden *computer flaw known to an intruder*, or a hidden computer mechanism (usually software) installed by an intruder, *who can activate the trap door to gain access* to the computer without being blocked by security services or mechanisms.

Trojan horse - A computer *program that appears to have a useful function*, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Virus - A hidden, *self-replicating section of computer software*, usually malicious logic, that *propagates by infecting* (i.e., inserting a copy of itself into and *becoming part of) another program.* A virus cannot run by itself; it requires that its host program be run to make the virus active.

Worm - A computer *program* that can run independently, *can propagate a complete working version of itself* onto other hosts on a network, and may consume computer resources destructively.

More types of malicious code exist…   [cf. http://www.ietf.org/rfc/rfc2828.txt]

C) Data Level of Vulnerabilities / Threats

- How valuable is your data?
  - Credit card info vs. your home phone number
  - Source code
  - Visible data vs. context
    - „2345" -> Phone extension or a part of SSN?

- Adequate protection
  - Cryptography
    - Good if intractable for a long time
- Threat of Identity Theft
  - Cf. Federal Trade Commission: http://www.consumer.gov/idtheft/ \

Identity Theft

- Cases:
  - Credit card skimmers plus drivers license, Florida
  - Faked social security and INS cards $150-$250
  - Used 24 aliases – used false id to secure credit cards, open mail boxes and bank accounts, cash fraudulently obtained federal income tax refund checks, and launder the proceeds
  - Bank employee indicted for stealing depositors' information to apply over the Internet for loans
  - $7M loss, Florida: Stole 12,000 cards from restaurants via computer networks and social engineering

Types of Attacks on Data CIA

- Disclosure
  - Attack on data *confidentiality*

- Unauthorized modification / deception
  - E.g., providing wrong data (attack on data *integrity*)

- Disruption
  - DoS (attack on data *availability*)

- Usurpation
  - Unauthorized use of services (attack on data *confidentiality*, *integrity* or *availability*)

Ways of Attacking Data CIA

- Examples of Attacks on Data Confidentiality
  - Tapping / snooping

- Examples of Attacks on Data Integrity
  - Modification: salami attack -> little bits add up
    - E.g/ „shave off" the fractions of cents after interest calculations
  - Fabrication: replay data -> send the same thing again
    - E.g., a computer criminal replays a salary deposit to his account

- Examples of Attacks on Data Availability
  - Delay vs. „full" DoS

- Examples of Repudiation Attacks on Data:
  - Data origin repudiation: „I never sent it"
    - Repudiation = refusal to acknowledge or pay a debt or honor a contract
  - Data receipt repudiation: „I never got it"

D) Vulnerab./Threats at Other Exposure Points

- Network vulnerabilities / threats
  - Networks multiply vulnerabilties and threats, due to:
    - their complexity => easier to make design/implem./usage mistakes
    - „bringing close" physically distant attackers
  - Esp. wireless (sub)networks

- Access vulnerabilities / threats
  - Stealing cycles, bandwidth
  - Malicious physical access
  - Denial of access to *legitimate* users

- People vulnerabilities / threats
  - Crucial weak points in security
    - too often, the *weakest* links in a security chain
  - Honest insiders subjected to skillful social engineering
  - Disgruntled employees
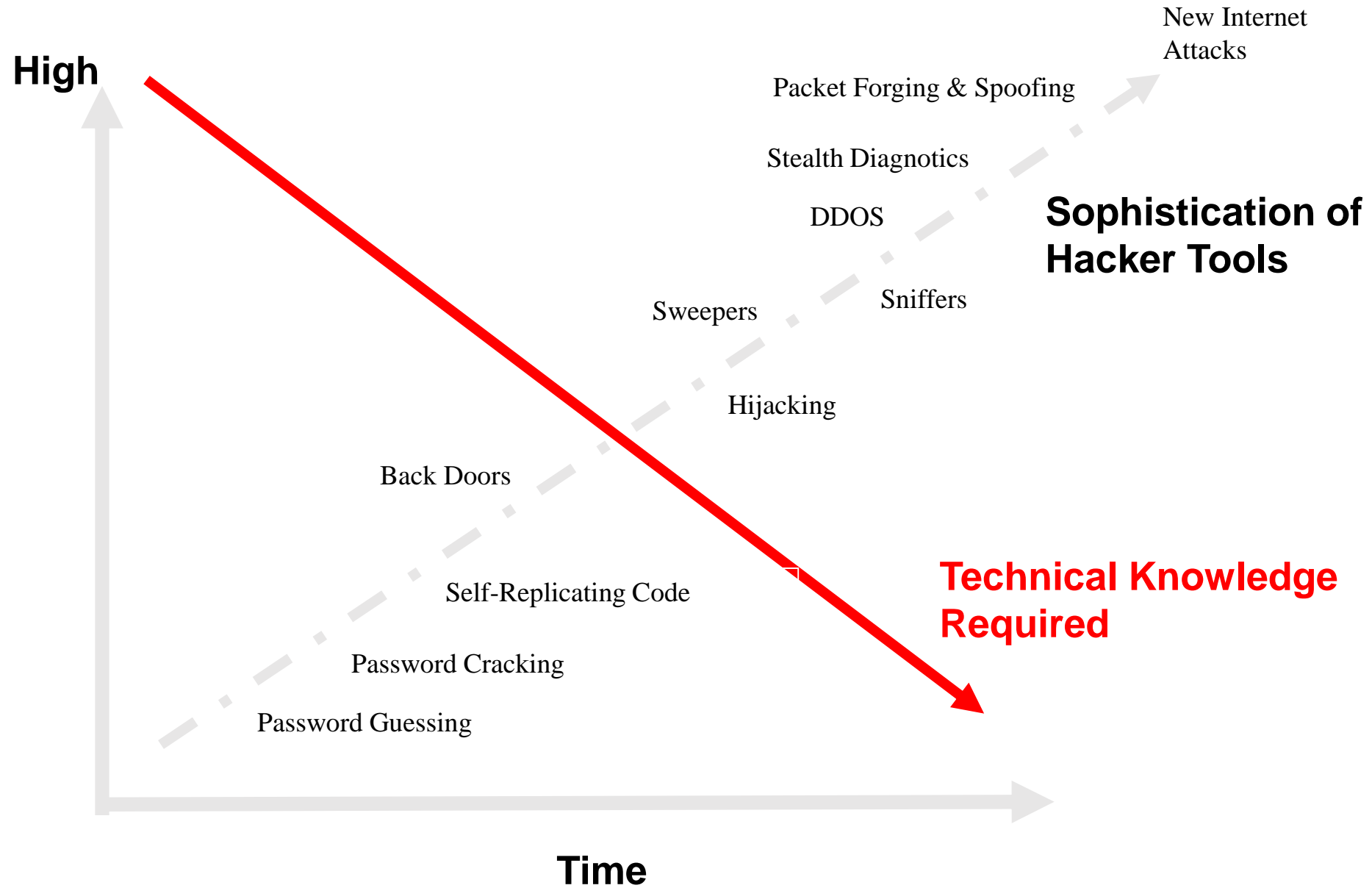
5. Attackers

- Attackers need MOM
  - Method
    Skill, knowledge, tools, etc. with which to pull off an attack
  - Opportunity
    Time and access to accomplish an attack
  - Motive
    Reason to perform an attack

Types of Attackers

- Types of Attackers - Classification 1
    - Amateurs
        - Opportunistic attackers   (use a password they found)
        - Script kiddies
    - Hackers - nonmalicious
        - In broad use beyond security community: also malicious
    - Crackers – malicious
    - Career criminals
    - State-supported spies and information warriors

- Types of Attackers - Classification 2 (cf. before)
    - Recreational hackers / Institutional hackers
    - Organized criminals / Industrial spies / Terrorists
    - National intelligence gatherers / Info warriors

Example: Hacking As Social Protest

- Hactivism

- Electro-Hippies

- DDOS attacks on government agencies

- SPAM attacks as "retaliation"

High

New Internet
Attacks

Packet Forging & Spoofing

Stealth Diagnotics

DDOS

**Sophistication of
Hacker Tools**

Sniffers

Sweepers

Hijacking

Back Doors

**Technical Knowledge
Required**

Self-Replicating Code

Password Cracking

Password Guessing

Time

6. Reacting to an Exploit

Exploit = successful attack

- Report to the vendor first?

- Report it to the public?
  - What will be public relations effects if you do/do not?

- Include source code / not include source code?

- Etc.

"To Report or Not To Report:" Tension between Personal Privacy and Public Responsibility

An info tech company will typically lose between ten and one hundred times more money from shaken consumer confidence than the hack attack itself represents if they decide to prosecute the case.

Computer Forensics
Against Computer Crime

- Technology

- Law Enforcement

- Individual and Societal Rights

- Judiciary

- …

7. Methods of Defense

- Five basic approaches to defense of computing systems

  - Prevent attack
    - Block attack / Close vulnerability
  - Deter attack
    - Make attack harder   (can't make it impossible ☹)
  - Deflect attack
    - Make another target more attractive than this target
  - Detect attack
    - During or after
  - Recover from attack

A) Controls

- Castle in Middle Ages
  - Location with natural obstacles
  - Surrounding moat
  - Drawbridge
  - Heavy walls
    - Arrow slits
    - Crenellations
  - Strong gate
    - Tower
  - Guards / passwords

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

- Medieval castles
  - location (steep hill, island, etc.)
  - moat / drawbridge / walls / gate / guards /passwords
  - another wall / gate / guards /passwords
  - yet another wall / gate / guards /passwords
  - tower / ladders up
- Multiple controls in computing systems can include:
  - system perimeter – defines „inside/outside"
  - preemption – attacker scared away
  - deterrence – attacker could not overcome defenses
  - faux environment (e.g. honeypot, sandbox) – attack deflected towards a worthless target (but the attacker doesn't know about it!)
- →Note layered defense /
  - multilevel defense / defense in depth (ideal!)

A.1) Controls: Encryption

- Primary controls!

- Cleartext scambled into ciphertext (enciphered text)

- Protects CIA:
  - confidentiality – by „masking" data
  - integrity – by preventing data updates
    - e.g., checksums included
  - availability – by using encryption-based protocols
    - e.g., protocols ensure availablity of resources for different users

A.2) Controls: Software Controls

- Secondary controls – second only to encryption

- Software/program controls include:
  - OS and network controls
    - E.g. OS: sandbox / virtual machine
    - Logs/firewalls, OS/net virus scans, recorders

  - independent control programs (whole programs)
    - E.g. password checker, virus scanner, IDS

  - internal program controls (part of a program)
    - E.g. read/write controls in DBMSs

- Considerations for Software Controls:
  - Impact on user's interface and workflow
    - E.g. Asking for a password too often?

A.3) Controls: Hardware Controls

- Hardware devices to provide higher degree of security
  - Locks and cables (for notebooks)
  - Smart cards, dongles, hadware keys, …
  - …

A.4) Controls: Policies and Procedures

- Policy vs. Procedure
  - Policy: *What* is/what is not allowed
  - Procedure: *How* you enforce policy

- Advantages of policy/procedure controls:
  - Can replace hardware/software controls
  - Can be least expensive
    - Be careful to consider *all* costs
      - E.g. help desk costs often ignored for for passwords (=> look cheap but migh be expensive)

- Policy - must consider:
  - Alignment with users' legal and ethical standards

  - Probability of use (e.g. due to inconvenience)
    - Inconvenient: 200 character password,
      - change password every week
    - (Can be) good: biometrics replacing passwords

  - Periodic reviews
    - As people and systems, as well as their goals, change

A.5) Controls: Physical Controls

- Walls, locks

- Guards, security cameras

- Backup copies and archives

- Cables an locks (e.g., for notebooks)

- Natural and man-made disaster protection
  - Fire, flood, and earthquake protection
  - Accident and terrorism protection

- ...

B) Effectiveness of Controls

- Awareness of problem
  - People convined of the need for these controls
- Likelihood of use
  - Too complex/intrusive security tools are often disabled
- Overlapping controls
  - >1 control for a given vulnerability
    - To provide layered defense – the next layer compensates for a failure of the previous layer
- Periodic reviews
  - A given control usually becomess less effective with time
  - Need to replace ineffective/inefficient controls with better ones

8. Principles of Computer Security

- ## Principle of Easiest Penetration

  An intruder must be expected to use any available means of penetration.

  The penetration may not necessarily be by the most obvious means, nor is it necessarily the one against which the most solid defense has been installed.

- ## Principle of Adequate Protection

  Computer items must be protected to a degree consistent with their value and only until they lose their value.

- **Principle of Effectiveness**

  Controls must be used—and used properly—to be effective.

  They must be efficient, easy to use, and appropriate.

- **Principle of Weakest Link**

  Security can be no stronger than its weakest link.

  Whether it is the power supply that powers the firewall or the operating system under the security application or the human, who plans, implements, and administers controls, a failure of any control can lead to a security failure.