CENG 374E - INTRODUCTION TO COMPUTER SECURITY

Prof. Dr. Şeref SAĞIROĞLU
Gazi University
Engineering Faculty
Computer Engineering Department
Maltepe/Ankara

SS@gazi.edu.tr
http://w3.gazi.edu.tr/~ss

CENG 374E - INTRODUCTION TO COMPUTER SECURITY

COURSE OUTLINE
&
INTRODUCTION

Why is Computer Security Important?

- Most information is ‘computerized’.
- Just as we protect physical belongings, we must also protect digital belongings.
- If we don’t, we are vulnerable to
  - Financial loss
  - Psychological damage
  - Physical damage

OK, But Who/What Can We Trust?

Nothing / Nobody (at least not completely)

- Nothing in the cyber world should be trusted.
- But we still want to think that we can trust the technologies we use.

This is the dilemma of computer security.

Erosion of Trust

Systems we use every day, websites containing our information, critical databases are vulnerable to attacks.

Recently we heard about:

- Edward Snowden and NSA wiretaps
- Illegal recordings at home and abroad
- iCloud attacks

Nobody is Safe

Cisco Annual Security Report:

- “100 percent of business networks analyzed by Cisco have traffic going to websites that host malware.”
- Most of them don’t even know it.

It’s Becoming More Complicated

Cisco Annual Security Report

These factors complicate security:

- Emergence of any-to-any infrastructure
- Growing number of Internet-enabled devices
- Trends such as cloud computing and mobility
- Criminals getting more sophisticated and resourceful

Smartphones are Dangerous!

- Another way for security to be compromised.
- Many users download apps without thinking about security.
- Data is backed up on the cloud (often automatically).
- Cloud is fundamentally insecure.

Cloud Traffic is Growing

- Cisco projects that cloud network traffic will grow more than threefold by the years 2000.
- Cloud redefines how and where data is stored, moved and accessed.
- Lack of info about how cloud vendors ensure security.

Are We Helpless?

Not quite.

- The weakest link for security is the human factor.
- Education and awareness can improve security.
- Plus we have many tools to help us.

Why Work on Computer Security?

Because this field is critical now and will stay so in the future.

Security Talent Shortage:

- Cisco ASR states that “It’s estimated that by the years 2000, the industry will still be short more than a million security professionals across the globe.”

Information Security Fundamentals

InfoSec is defined in ISO 27000 as:

“Preservation of Confidentiality, Integrity and Availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.”

The CIA triad of InfoSec: fundamentals, goals, attributes…

CIA of InfoSec: Confidentiality

Keeping information SECRET

- Only authorized parties can access information.
- No one else should see it or have access.

Examples: sensitive documents for a company, state secrets, military plans, texts on your phone

Encryption is a tool used to preserve confidentiality (more on encryption later in the course)

CIA of InfoSec: Integrity

Keeping information UNCHANGED

- Guarantee that information has not been changed or damaged.
- If it was changed, it will be known.
- Does NOT guarantee confidentiality.

Example: Making sure that message sent = message received.

Checksums and hash functions are used for integrity (More on these later)

CIA of InfoSec: Availability

Keeping information **ACCESSIBLE**

- Percentage of time (or probability) that information is available to authorized parties.

Example: ÖSYM website must be available.

A common attack on availability is **Denial of Service** (DoS – more on this later)

CIA of InfoSec: More Examples

- Your mother read your emails → Loss of

  Confidentiality

- Your roommate opened your credit card statement → Loss of

  Confidentiality

- University website is down and you cannot check your class schedule → Loss of

  Availability

CIA of InfoSec: More Examples

- Your brother took a message for you but forgot who left it (or wrote down the name wrong)

→ Loss of Integrity

- Your father read AND deleted a text you received

→ Loss of Confidentiality AND Integrity

- Hackers hacked a government website AND corrupted encrypted password records

→ Loss of Integrity AND Availability

Other InfoSec Attributes

Authenticity: Being REAL

- Are you who you claim to be? Is that message really from him?
- Digital signatures are used for authenticity (more on this later).

Non-repudiation: You CANNOT DENY that the information was generated by you.

- Integrity plus authenticity
- Digital signatures are also used for non-repudiation.

Vulnerability

ISO 27005 Definition: "*A weakness of an asset or group of assets that can be exploited by one or more threats*"

ISO 27005 Classification:

- Hardware: Lack of physical protection, temperature, humidity etc.
- Software: Memory violations, input validation errors etc.
- Personnel: Human factors, flawed recruitment, inadequate awareness
- Site: Susceptibility to power outage or disasters such as fire
- Network: Unprotected communication lines, insecure architecture
- Organization: Lack of plans, procedures, audits etc.

Threat

ISO 27005 Definition: *“A potential cause of an incident, that may result in harm of systems and organization”*

Any danger that may exploit a vulnerability to cause harm

- Threat is not the same thing as an attack.

Intentional threats: Spies, crackers, criminal organizations etc.

Accidental threats: Computer crashes, natural disasters etc.

Classification and more examples of threats: Next lecture

Attack

Intentional threat → Attack

IETF definition: “an assault on system security that derives from an intelligent threat”

- Active: change resources or affect operation
- Passive: learn information without changing

- Insider: Attack by authorized user
- Outsider: Attack by unauthorized user

Why Do Attackers Attack?

In criminal law, three things must be present for a crime to occur:

- Means: Ability to commit the crime
- Motive: Reason for the crime
- Opportunity: Chance to commit the crime

Examples:

- I have a gun. He killed my father. I found him alone.
- I can unlock doors. I need money and you’re rich. You’re not home.

Cyber Crime

Means:

- Criminals are becoming more experienced and better organized.
- They find new ways to break security, defenders respond.
- Even if you're not a computer expert or hacker, you have the ability to commit cyber crime.
    - Crimeware-as-a-service

Cyber Crime

Motive:

- Financial gain
- Stealing critical data
- Disrupting service
- Destroying infrastructure
- Reputation

Cyber Crime

Opportunity:

- Cyber world is full of vulnerabilities.
- Both accidental vulnerabilities or intentional "backdoors"
- Many users are uneducated.

IT Risk

Risk is the likelihood that a threat will exploit a vulnerability to cause harm to a valuable asset.

Harm can be loss of confidentiality, integrity, availability, or some other security property.

A countermeasure is a way to prevent a threat from causing harm.

IT Risk

Vulnerabilities and threats increase risk, countermeasures reduce risk.

Risk = Likelihood × Impact = Probability × Magnitude

can be extended as

Risk = (Vulnerability × Threat / Countermeasures) × Asset value

IT Risk

Threat factors: skill, motive, opportunity, size

Vulnerability factors: ease of discovery, ease of exploit, awareness, intrusion detection

Impact factors: technical impact (loss of security attributes), business impact (financial loss, reputation damage, privacy violation)

Countermeasures: Security Controls

- Physical: Controlling access to physical facilities
  - Locks on doors
  - Alarms (burglar, smoke etc.)
  - Video cameras
  - Guards
- Logical (technical): Software use
  - Passwords, firewalls, antivirus etc.
- Administrative (procedural): Policies and standards

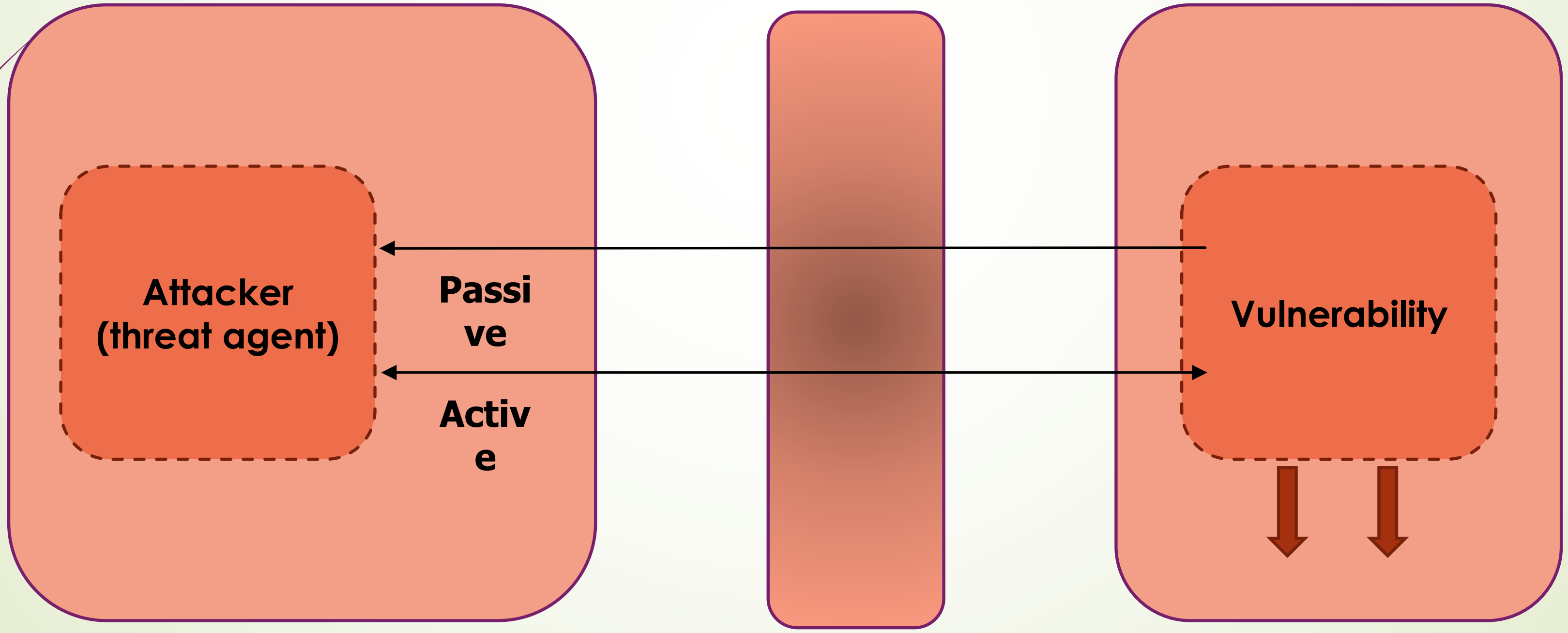
Security Concepts in a Diagram

(Adapted from RFC 2828)

Attack (threat action)

Countermeasure

Target (system resource)



Attacker (threat agent)

Passi
ve

Activ
e

Vulnerability

Threat Consequences

Defense in Depth

Combining different security controls into a layered defense mechanism

Do NOT trust a single line of defense.

“Hatt-ı müdafaa yoktur sath-ı müdafaa vardır.” M.K. Atatürk

Defense in Depth

Use multiple countermeasures together to increase security.

- Guards, locks, alarms, cameras etc. for physical security
- Passwords and other access control techniques for logical security
- Access policies for administrative security

If one line of defense is broken, there are others.

Risk Management

Risk: Probability that something harmful will happen to information

- Identifying vulnerabilities and threats to information
- Deciding on countermeasures to reduce risk
- Based on the value of the information to the organization

Risk management is a continuous effort.

- Vulnerabilities and threats are always changing.
- Countermeasures must also change accordingly.

Risk Management

- Effort for protection must be appropriate for the value of the asset.
- It is impossible to fully protect all resources at all times.

"If you try to defend everything, you defend nothing."

Frederick the Great of Prussia

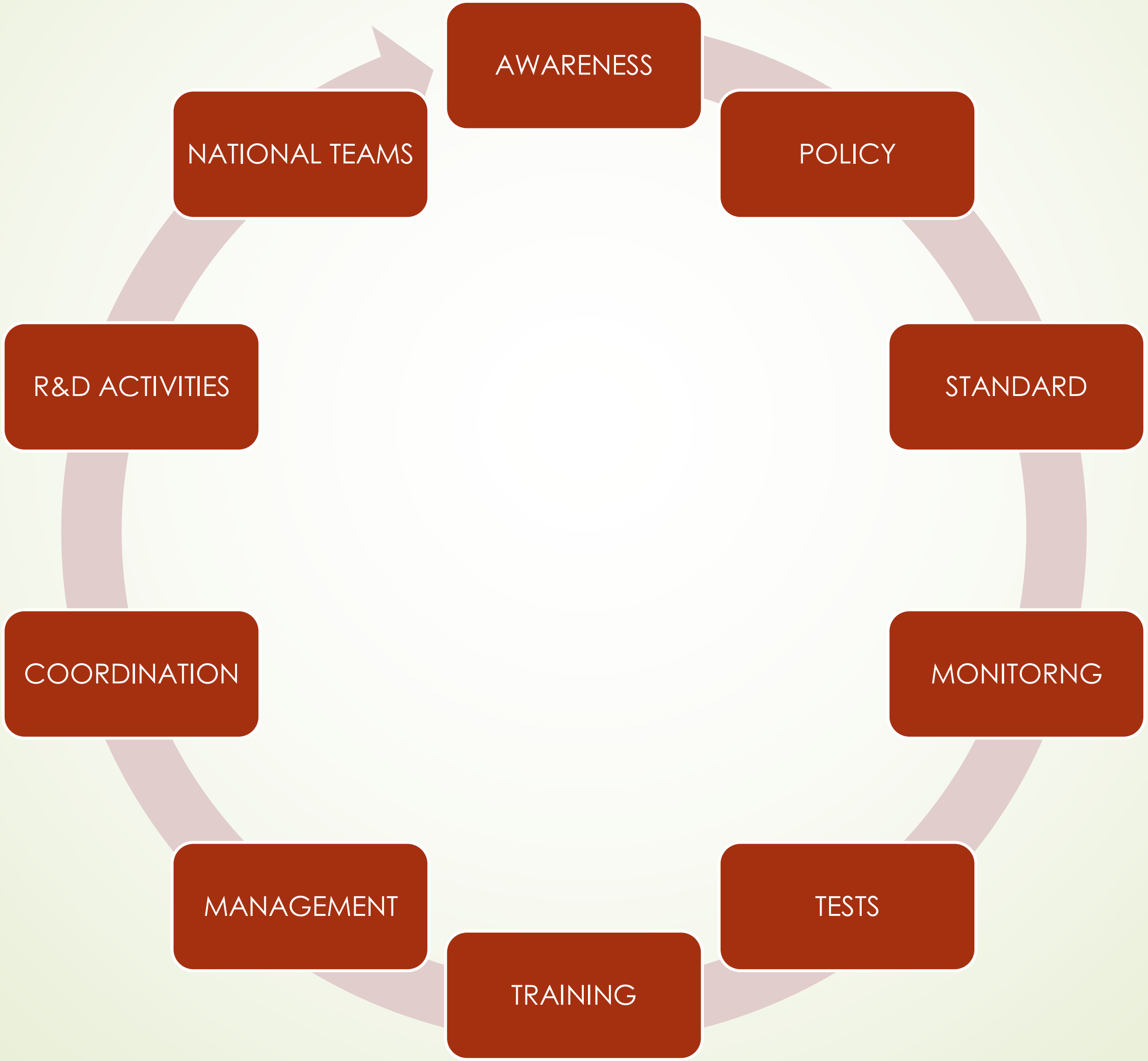
Risk Management

- a systematic process that organizations use to identify, assess, and mitigate risks to their digital assets, information systems, and data.
- involves understanding the threats and vulnerabilities that could impact an organization and implementing strategies to reduce or manage the risks.
  - 1. Identification of Risks
  - 2. Risk Assessment and Analysis
  - 3. Risk Mitigation and Treatment
  - 4. Implementation of Controls
  - 5. Monitoring and Review
  - 6. Documentation and Communication
- maintain a resilient posture against an ever-evolving threat landscape.

Summary: Lecture Outcomes

- Understand the meaning and importance of information and computer security
- Know the definitions and examples of all of these terms:
  - Confidentiality, Integrity, Availability, Authentication, Non-repudiation
  - Vulnerability, Threat, Risk, Countermeasure
  - Physical, Logical, Administrative security controls
  - Defense in Depth

SECURITY PERSPECTIVE



Summary: Building a security Perspectives

- involves several critical steps that combine understanding risk, implementing effective measures, and continuously evaluating security processes.
- Here's a general framework you might consider:
- **Risk Assessment (Identify Assets; Assess Threats and Vulnerabilities)**
- **Security Strategy Development (Set Objectives; Develop Policies and Procedures**)
- **Implementation of Security Measures (Physical Security; Cybersecurity; Personnel Security)**
- **Continuous Monitoring and Improvement (Monitor Security Systems; Incident Response and Recovery; Regular Updates and Training)**
- **Legal and Compliance (Stay Informed on Legal Requirements; Ethical Considerations)**
- **Community and Industry Collaboration (Engage with Others)**
- not a one-time task but a continuous process that adapts to new threats and technologies.

Q&A