Lecture 2: Introduction to Computer Security

Computer Security Overview

- The NIST Computer Security Handbook defines the term **Computer Security** as:

  "The protection afforded to an automated information system in order to attain the applicable objectives of preserving the **integrity**, **availability** and **confidentiality** of information system resources"

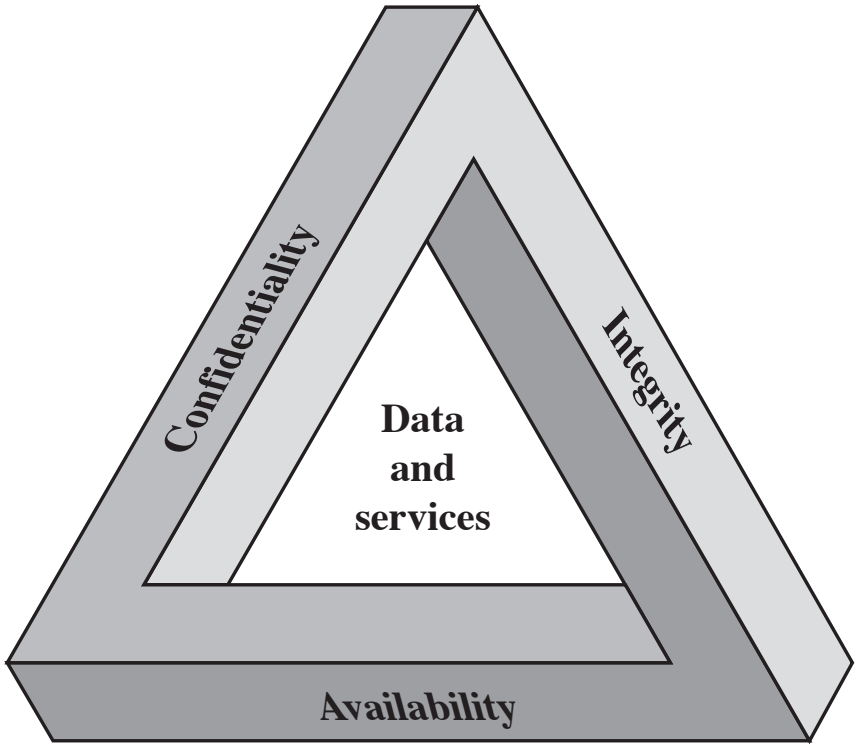
Overview

Translate in language we could understand…

- What assets do we need to protect?
- How are those assets threatened?
- What can we do to counter those threats?

Computer Security Overview

- The definition of **integrity**, **availability** and **confidentiality** (three key objectives of computer security)



Computer Security Overview

- Confidentiality:
  - Data confidentiality: assures that private or confidential information is not made available or disclosed to unauthorized individuals.
  - Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Computer Security Overview

- Integrity:
  - Data integrity: Assures that information and programs are changed only in a specified and authorized manner.
  - System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or unauthorized manipulation of the system.

Computer Security Overview

- Availability: Assures that systems work promptly and service is not denied to authorized users.

Example

- Confidentiality —An employee should not know the salaries of his colleagues
- Integrity —An employee should not be able to modify the employee's own salary
- Availability —Paychecks should be printed on time as stipulated by law

Examples

- The target coordinates of a missile should not be improperly disclosed
- The target coordinates of a missile should not be improperly modified
- When the proper command is issued the missile should fire

Levels of Impact

Low

The loss could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals

Moderate

The loss could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals

High

The loss could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals

Examples

- An organization of managing public information on its web server
  - Loss of integrity → ?
  - Loss of confidentiality→?
  - Loss of availability→?

Examples -2

- A law enforcement organization managing extremely sensitive investigative information
  - Loss of integrity→?
  - Loss of confidentiality→?
  - Loss of availability→?

Examples -3

- A power plant contains a SCADA (supervisory control and data acquisition) systems controlling the distribution of electric power for large military installation
  - Loss of integrity→?
  - Loss of confidentiality→?
  - Loss of availability→?

Computer Security Terminology

- **Adversary** (threat agent)
  - An entity that attacks, or is a threat to, a system.
- **Attack**
  - An assault on system security that derives from an intelligent threat; a deliberate attempt to evade security services and violate security policy of a system.
- **Countermeasure**
  - An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Computer Security Terminology

- **Risk**
  - An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
- **Security Policy**
  - A set of rules and practices that specify how a system or org provides security services to protect sensitive and critical system resources.
- **System Resource (Asset)**
  - Hardware, software, data, communication

Computer Security Terminology

- **Threat**
  - A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

- **Vulnerability**
  - Flaw or weakness in a system's design, implementation or operation and management that could be exploited to violate the system's security policy.

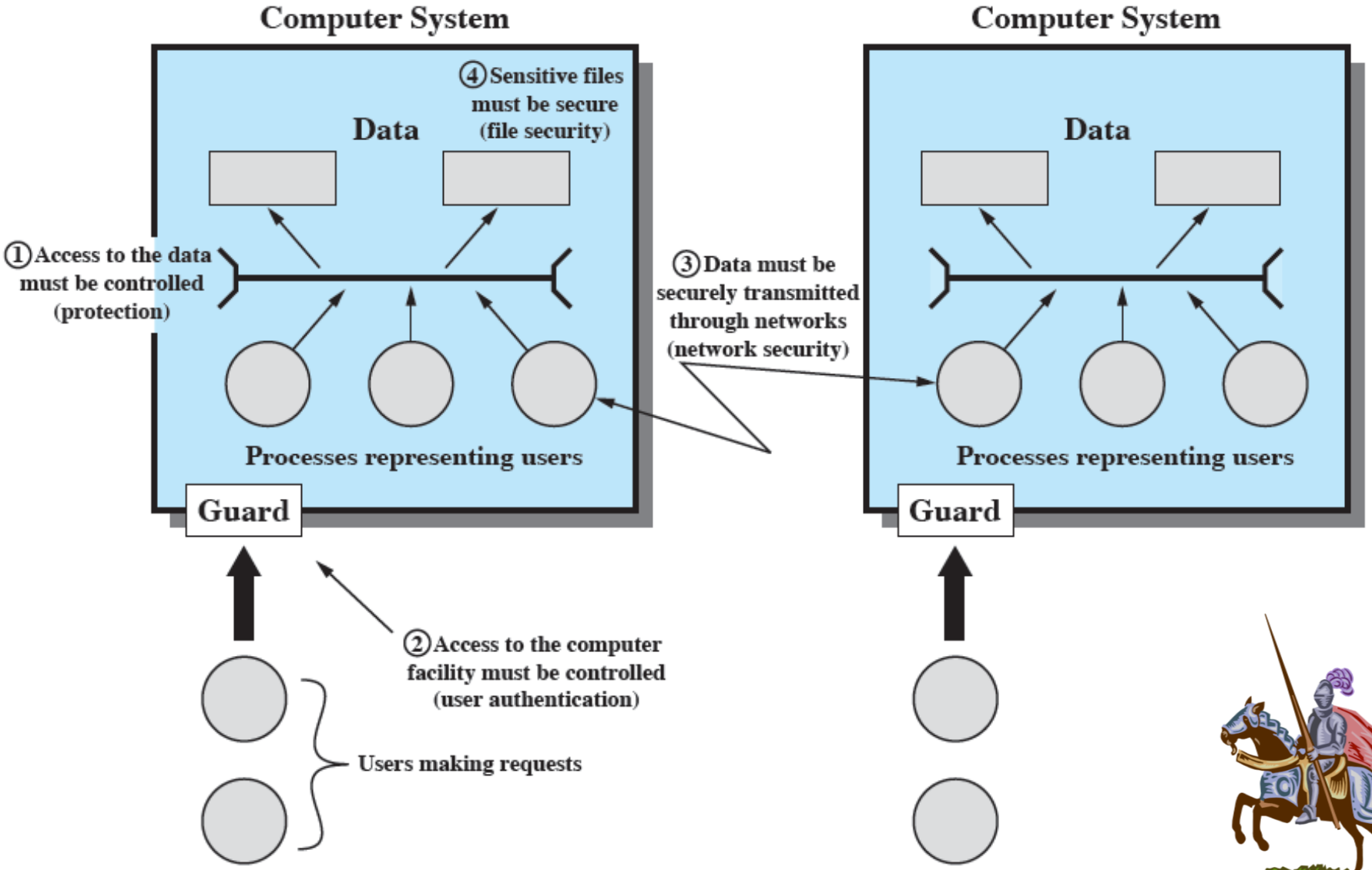
Vulnerabilities and Attacks

- vulnerabilities
  - leaky (loss of confidentiality)
  - corrupted (loss of integrity)
  - unavailable or very slow (loss of availability)
- attacks (threats carried out)
  - passive or active attempt to alter/affect system resources
  - insider or outsider

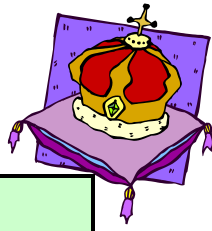
Attacks

- Passive attacks and active attacks
  - Passive attacks
    - Eavesdropping on, monitoring transmissions. (Email, file transfer, client/server exchanges)
  - Active attacks
    - Modification of transmitted data and attempts to gain unauthorized access to computer systems

Scope of Computer Security

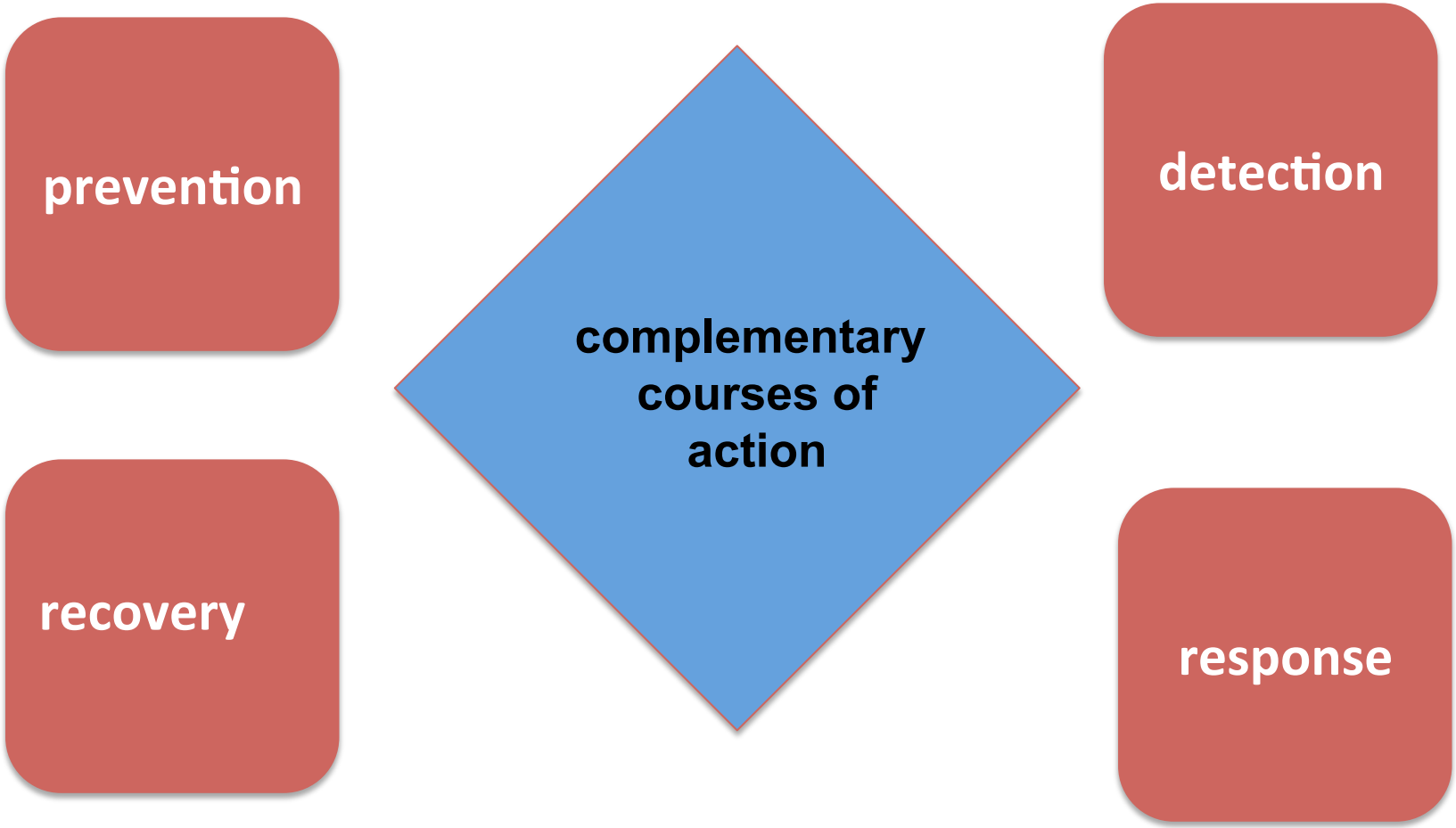


Scope of Computer Security

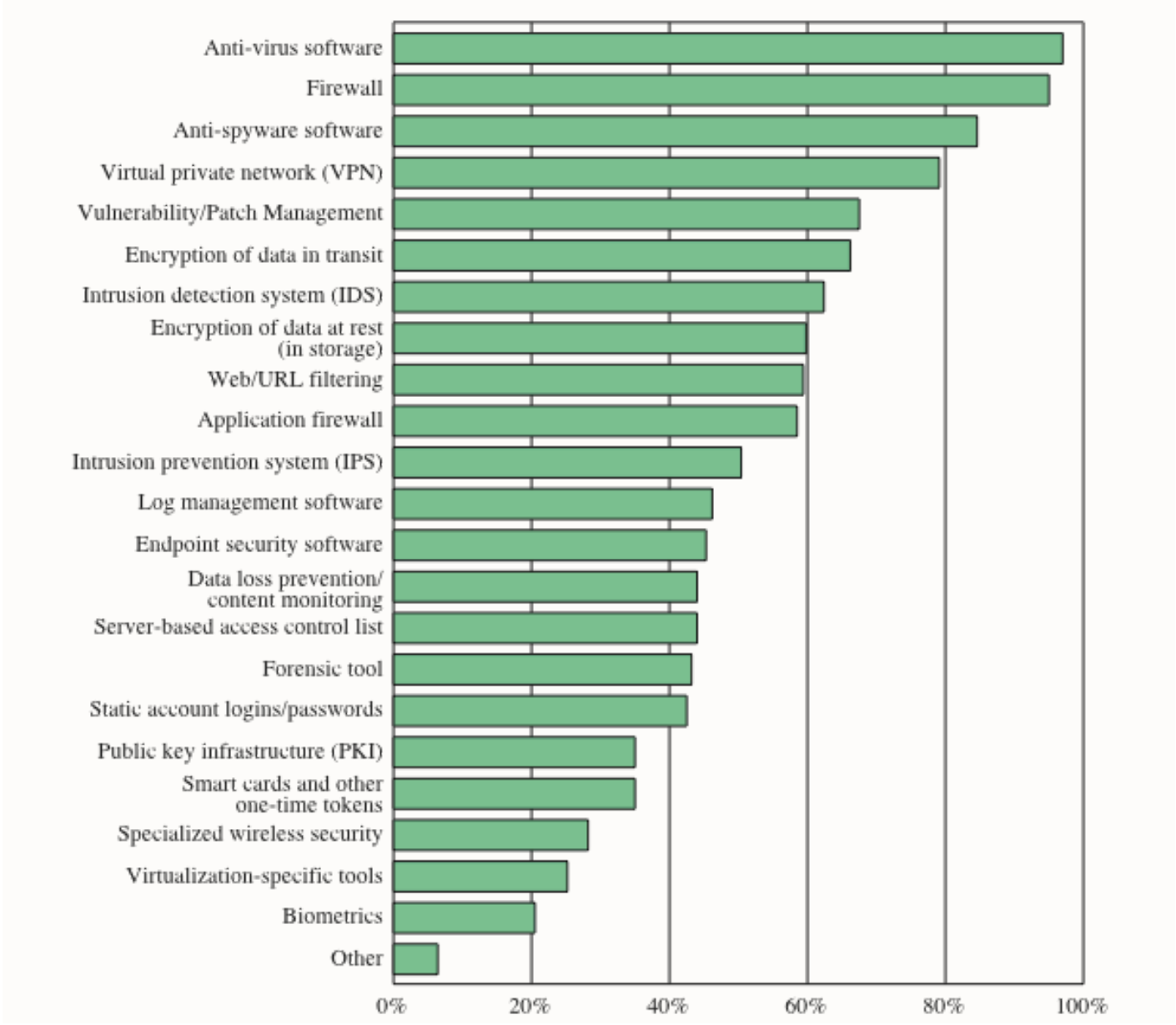


	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	Jamming
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Security Implementation



Security Technologies Used



Practice

```
DWORD dwRet =  IsAccessAllowed (…)

if (dwRet == ERROR_ACCESS_DENIED)  {
// security check failed.
//Inform unser that access is denied.
}  else  {
//security check OK.
}
```

Practice (Corrected)

```
DWORD dwRet = IsAccessAllowed(...);


if (dwRet == NO_ERROR) {
   // Secure check OK.
   // Perform task.
} else {
  // Security check failed.
  // Inform user that access is denied.
}
```

- Next Class
  - Chapter 3: User Authentication