

Computer Security Principles



MODULE 1

Overview : Definition

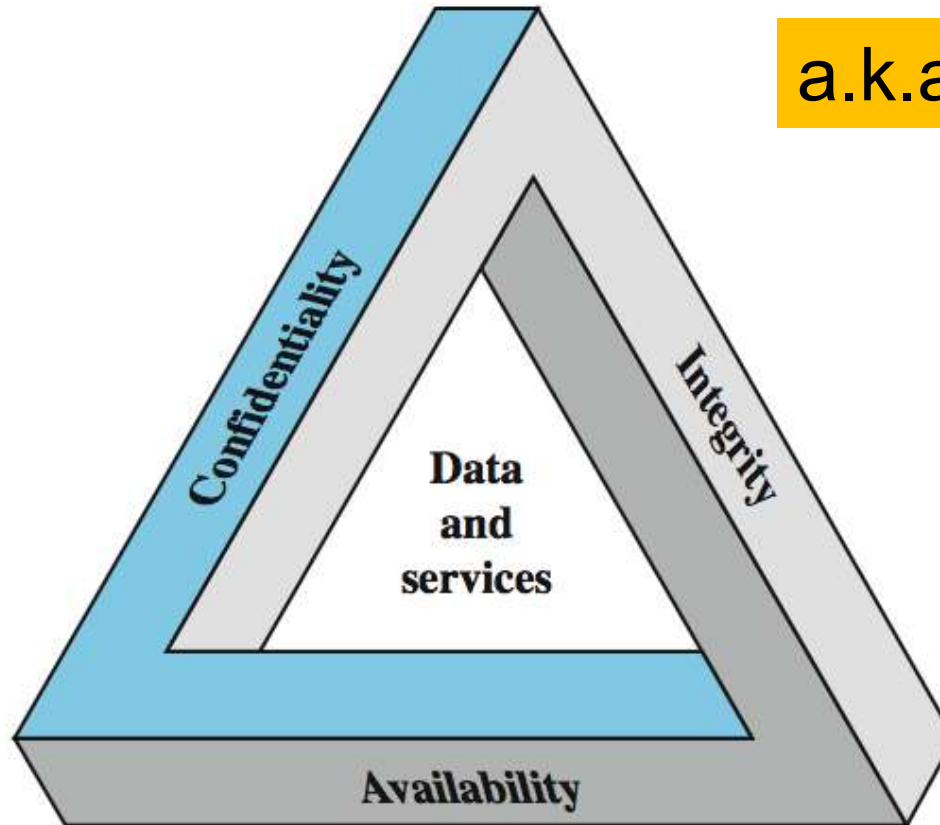
What are we protecting?

Computer Security: 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 (includes hardware, software, firmware, information/data, and telecommunications).

– NIST Computer Security Handbook

Key Security Concepts

a.k.a the CIA



Key Security Concepts



- **Confidentiality:**
- Preserving **authorized restrictions** on **information access and disclosure**, including means for protecting personal privacy and proprietary information.
- A loss of confidentiality is the unauthorized disclosure of information.

Think of it as → Keeping a secret, secret

Key Security Concepts : Confidentiality



Privacy – assures that data owners control who get to see/store/use data

Data confidentiality – assures private data stays private

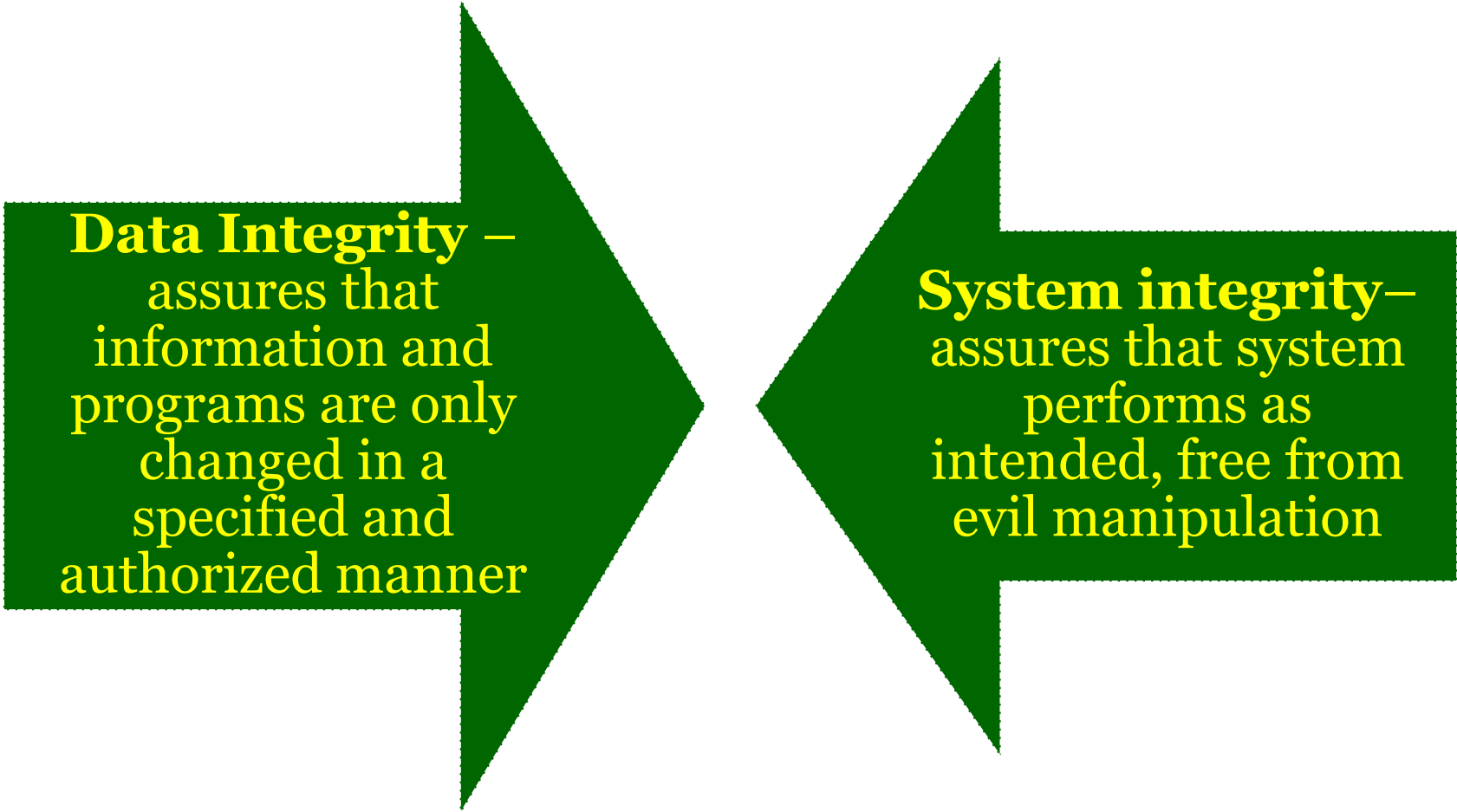
Key Security Concepts



- **Integrity:**
- Guarding against **improper** information **modification** or **destruction**, and includes ensuring information non-repudiation and authenticity.
- A loss of integrity is the unauthorized modification or destruction of information.

Think of it as → Ensuring the secret is in its original state.

Key Security Concepts: Integrity



Data Integrity –
assures that
information and
programs are only
changed in a
specified and
authorized manner

System integrity–
assures that system
performs as
intended, free from
evil manipulation

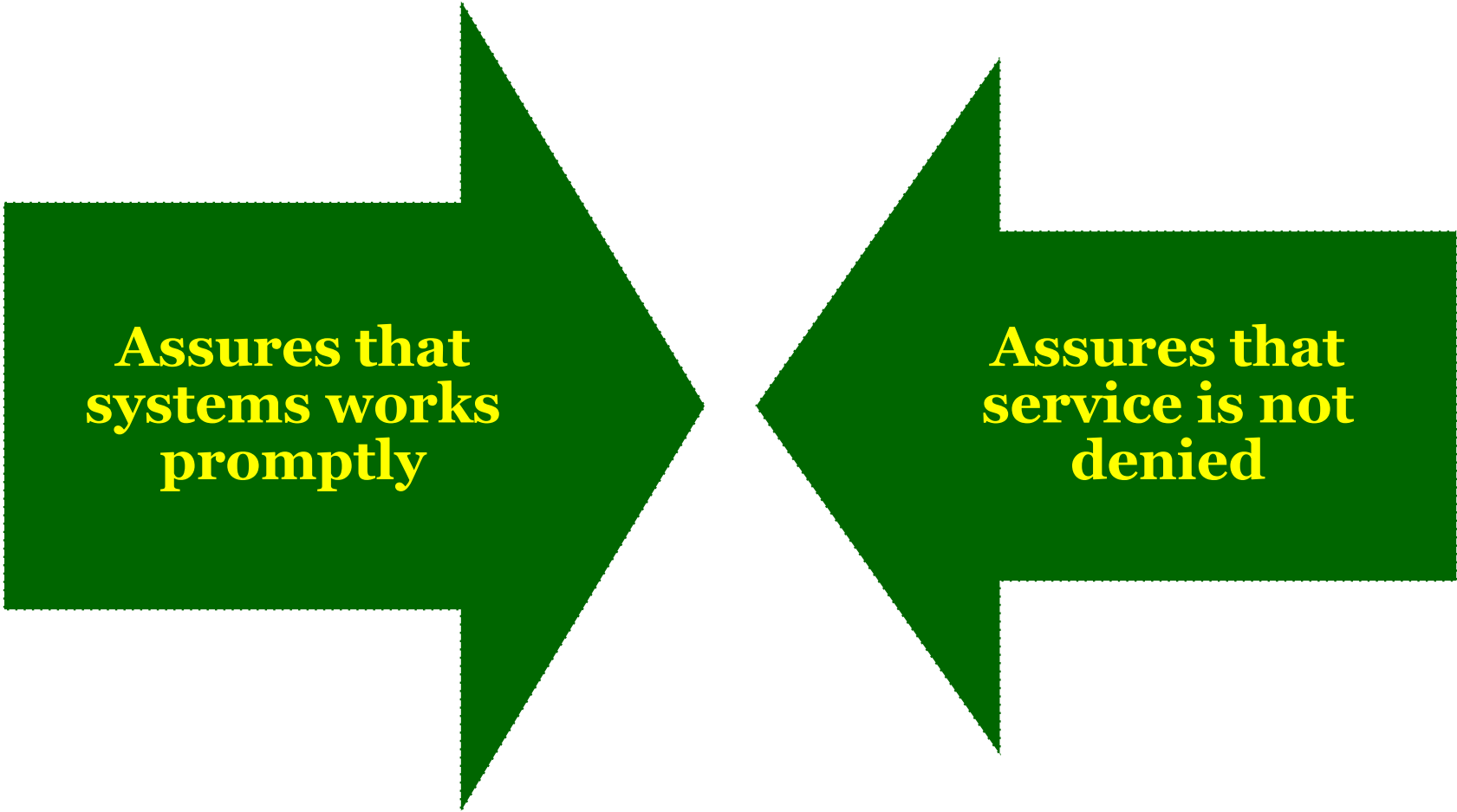
Key Security Concepts



- **Availability:**
- Ensuring timely and reliable access to and use of information.
- A loss of availability is the disruption of access to information system.

Think of it as → When you need it its always there.

Key Security Concepts: Availability



**Assures that
systems works
promptly**


**Assures that
service is not
denied**

Computer Security Challenges

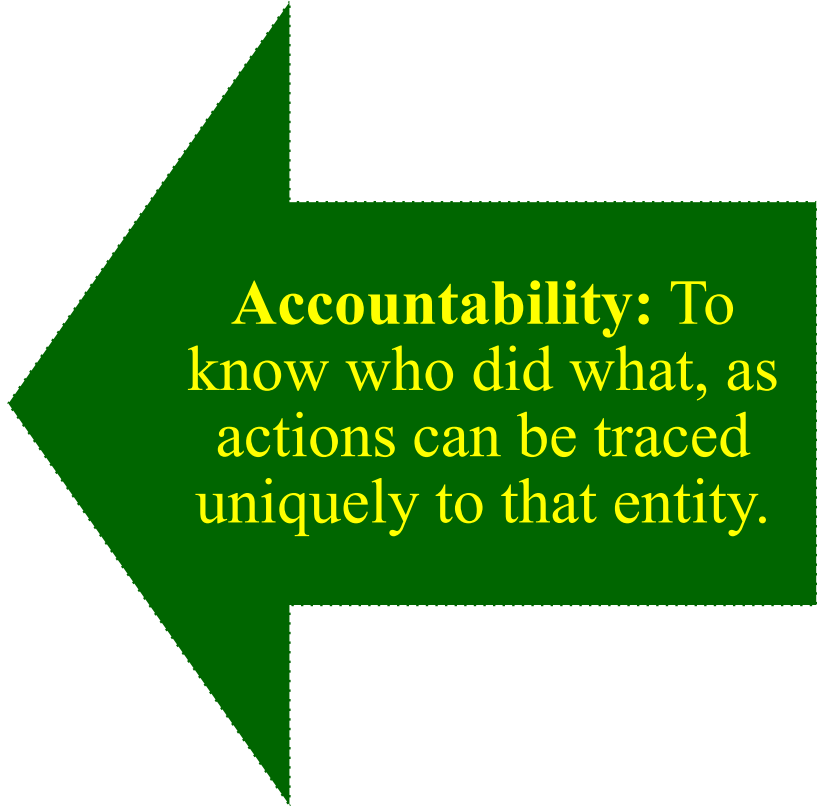


- Although the use of the CIA triad well established, some feel that extra concepts are needed to present a complete picture.
- Two of the most commonly mentioned are:
- **Authenticity:** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
- **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

Key Security Concepts: Extras



Authenticity: the entity is who they say they are → verified genuine and trusted



Accountability: To know who did what, as actions can be traced uniquely to that entity.

Computer Security Challenges



1. not simple
2. must consider potential attacks
3. involve algorithms and secret info
4. must decide where to deploy mechanisms
5. battle of wits between attacker / admin
6. not perceived on benefit until fails
7. requires regular monitoring
8. too often an after-thought
9. regarded as impediment to using system

Security Terminology



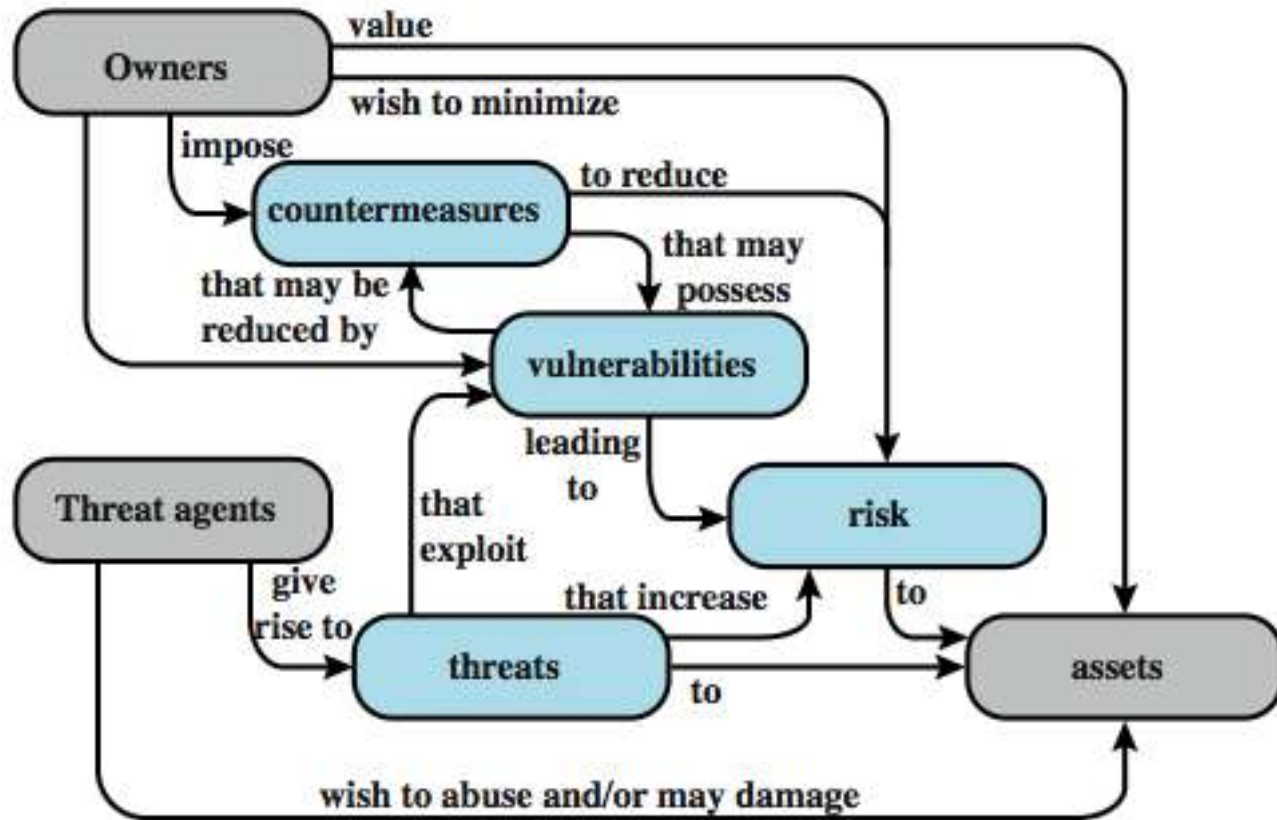
- **Adversary (threat agent)** - An entity that attacks, or is a threat to, a system.
- **Attack** -An assault on system security that derives from an intelligent threat; a deliberate attempt to evade security services and violate security policy of a system.
- **Countermeasure** - An action, device, 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.
- **Risk** - An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Security Terminology



- **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)** - Data; a service provided by a system; a system capability; an item of system equipment; a facility that houses system operations and equipment.
- **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.

Security Terminology Relationship



Vulnerabilities

General categories of vulnerabilities of a computer system

be corrupted

- loss of integrity

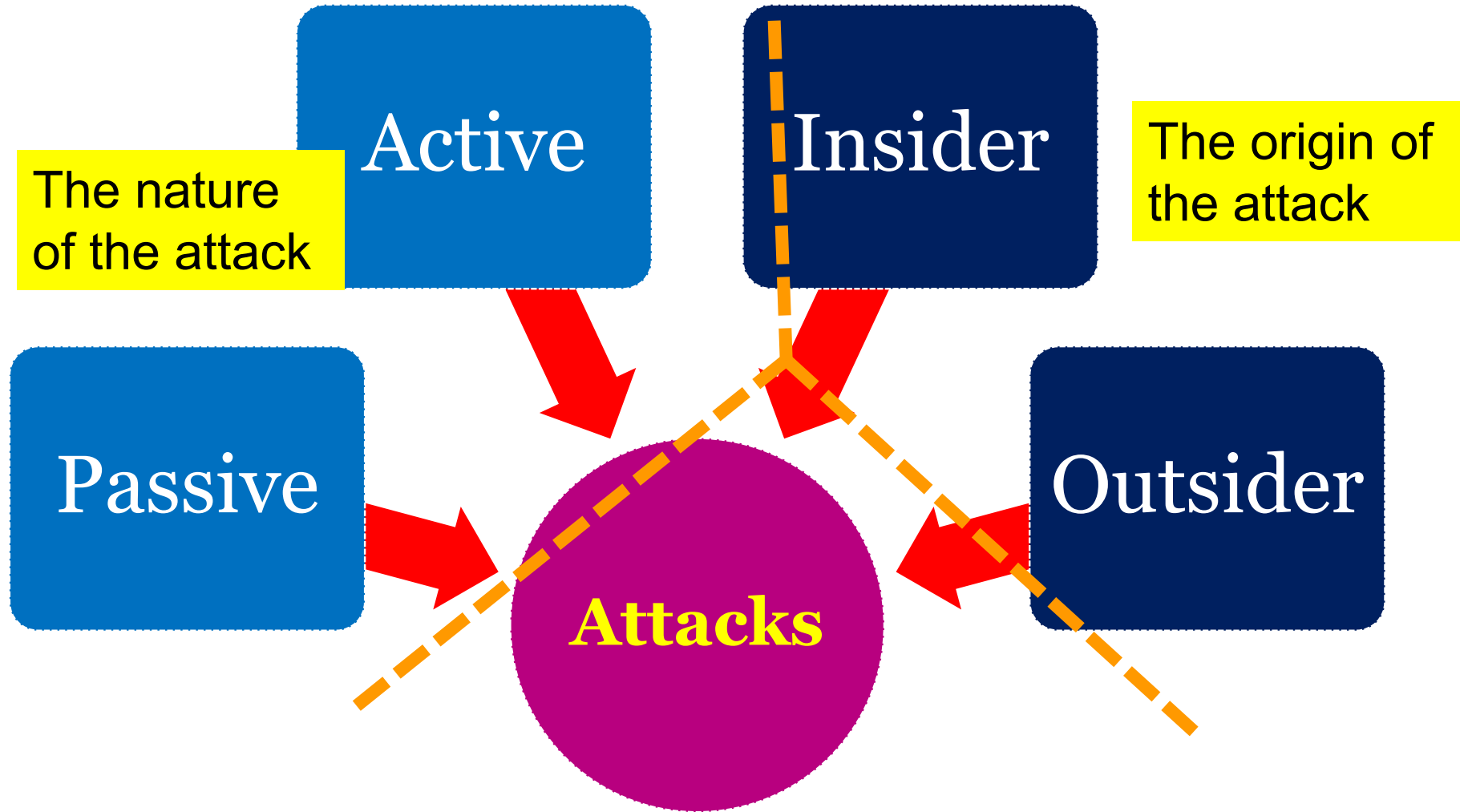
become leaky

- loss of confidentiality

become unavailable

- loss of availability

Attacks



Countermeasures

may result in new vulnerabilities

prevent

detect

recover

Threat Consequences

What are the consequences of attacks?

Someone unauthorized
can access/get your data

unauthorized
disclosure

You might believe false
information is the truth

deception

disruption

Your system not
working as it should

usurpation

Someone else gets
control of your system

Threat Consequences

What attacks can give these consequences?

exposure,
interception,
inference,
intrusion

unauthorized
disclosure

masquerade,
falsification,
repudiation

deception

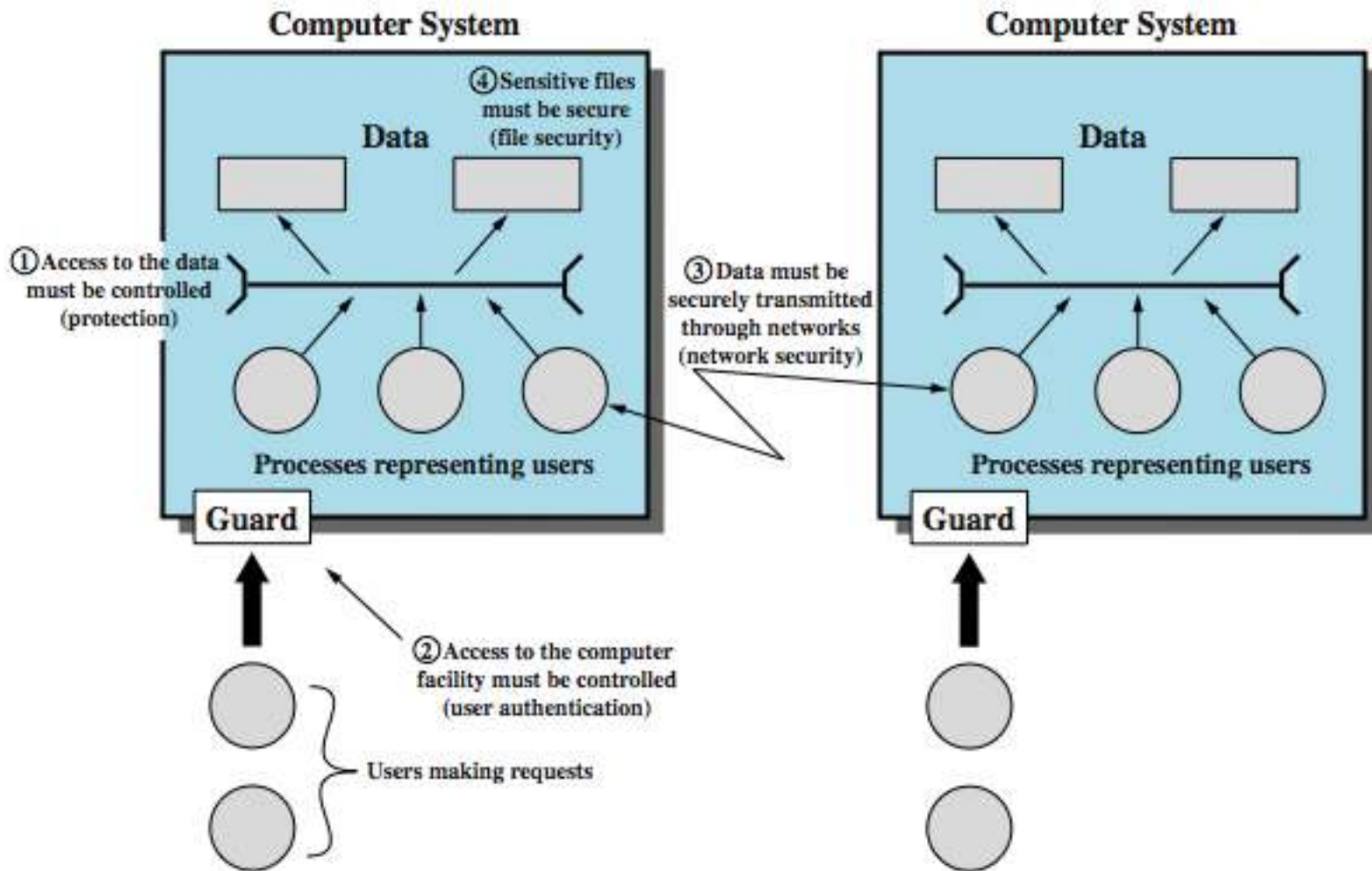
disruption

usurpation

incapacitation,
corruption,
obstruction

misappropriation,
misuse

Scope of Computer Security



Scope of Computer Security



- What are we protecting?
 - Assets
- What are these assets of a computer system?
 - Hardware,
 - software,
 - data,
 - communication lines and networks.

Assets : Hardware

Examples	Disk, ports, cards, power, server, external hard drive etc, cpu
Possible Threats (to CIA)	Destroyed, unauthorized memory, embedded trojan, theft, natural disaster, lost power, corrupting,
Possible counter measures	Guarded, locking, physical lock, combination locks, uninterrupted power supply , grills, access control, backup

Assets : Software

Examples	OS, database, system software, mobile application, browsers, applications,
Possible Threats (to CIA)	Unauthorized copying, host threats, rootkits, virus, worm, trojan horse, malware, adware, database threats, backdoor, cracking, DoS, unauthorized data modification,
Possible counter measures	Password, web proxy, encryption, antivirus, up to date, protocols, awareness training,

Assets : Data

Examples	files, student information, financial data, grading data, personal information,
Possible Threats (to CIA)	Access to it denied, spoofing, manipulation, phishing, information disclosure, denial of service, repudiation, sniffing, delete data, destroy
Possible counter measures	Password, encryption, authorization, digital signature, access control, backup, validate and filter,

Assets : Communication Lines

Examples	cables, messages, wireless, signals, bluetooth,
Possible Threats (to CIA)	Sniffing, eavesdropping, masquerade, cut the cable, Dos, spoofing, unauthorized traffic analysis
Possible counter measures	Encryption, password, digital signature, validate and filter

Network Security Attacks



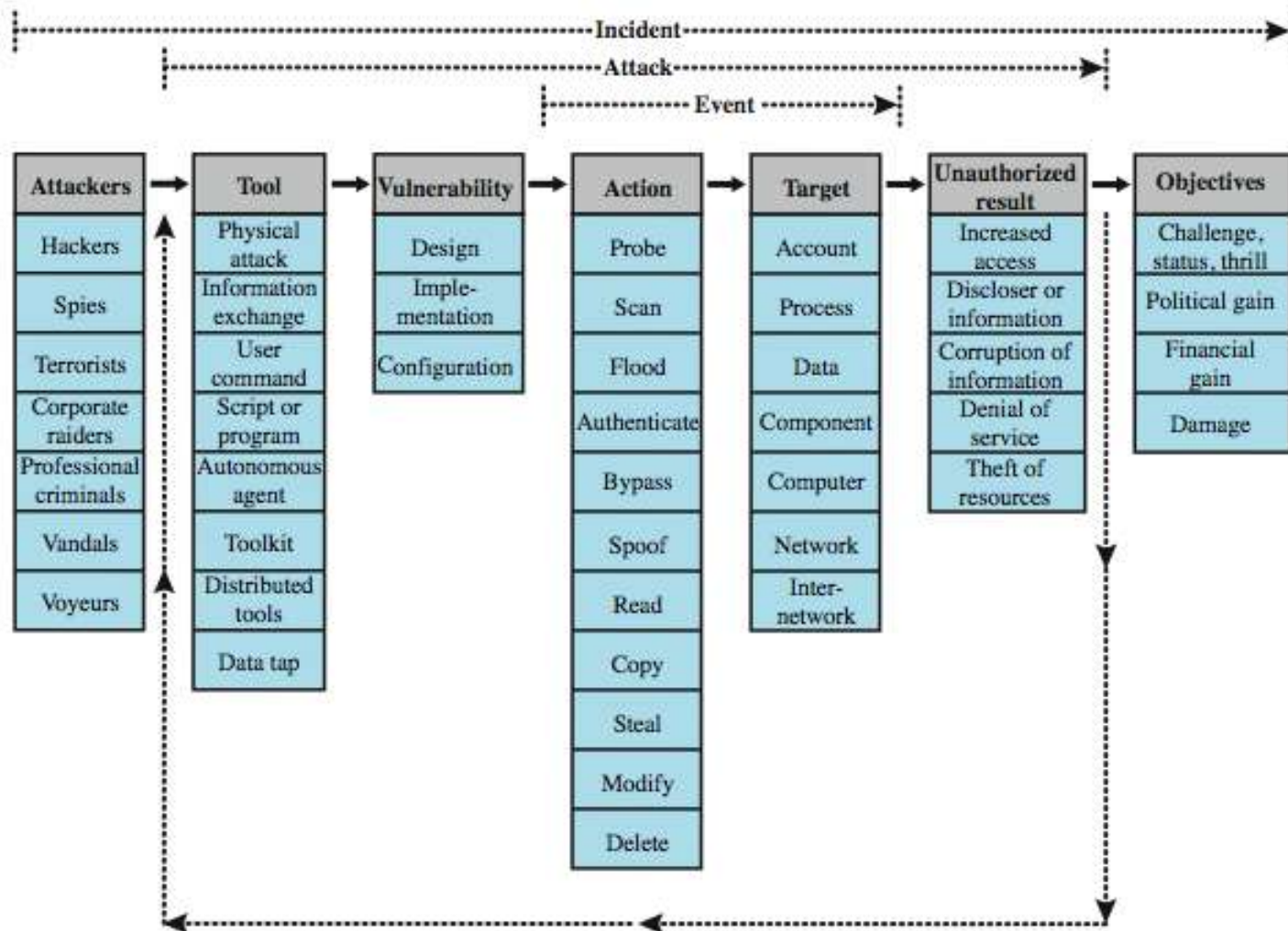
- classify as passive or active
- passive attacks are eavesdropping
 - release of message contents
 - traffic analysis
 - are hard to detect so aim to prevent
- active attacks modify/fake data
 - masquerade
 - replay
 - modification
 - denial of service
 - hard to prevent so aim to detect

Security Functional Requirements

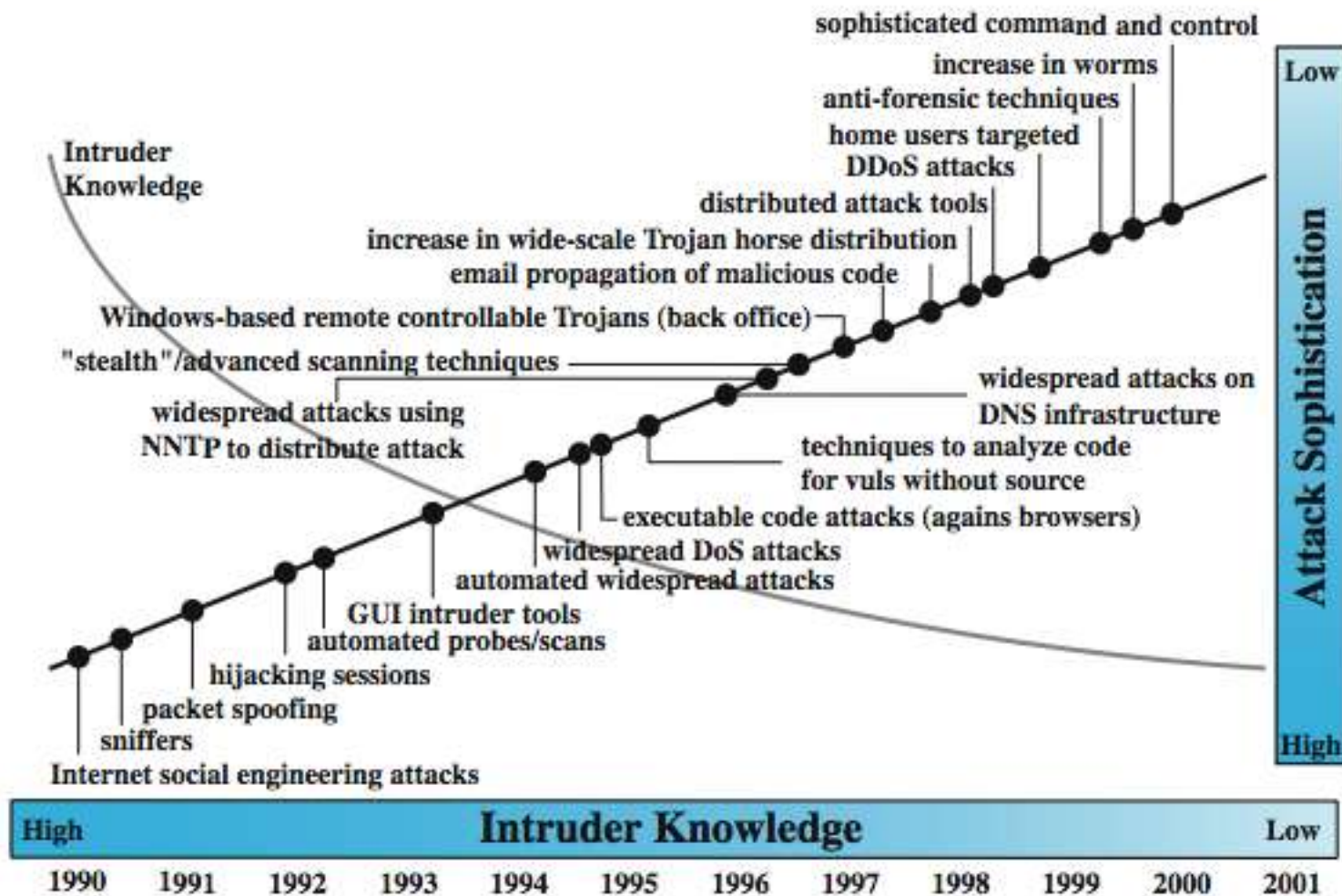


- technical measures:
 - access control; identification & authentication; system & communication protection; system & information integrity
- management controls and procedures
 - awareness & training; audit & accountability; certification, accreditation, & security assessments; contingency planning; maintenance; physical & environmental protection; planning; personnel security; risk assessment; systems & services acquisition
- overlapping technical and management:
 - configuration management; incident response; media protection

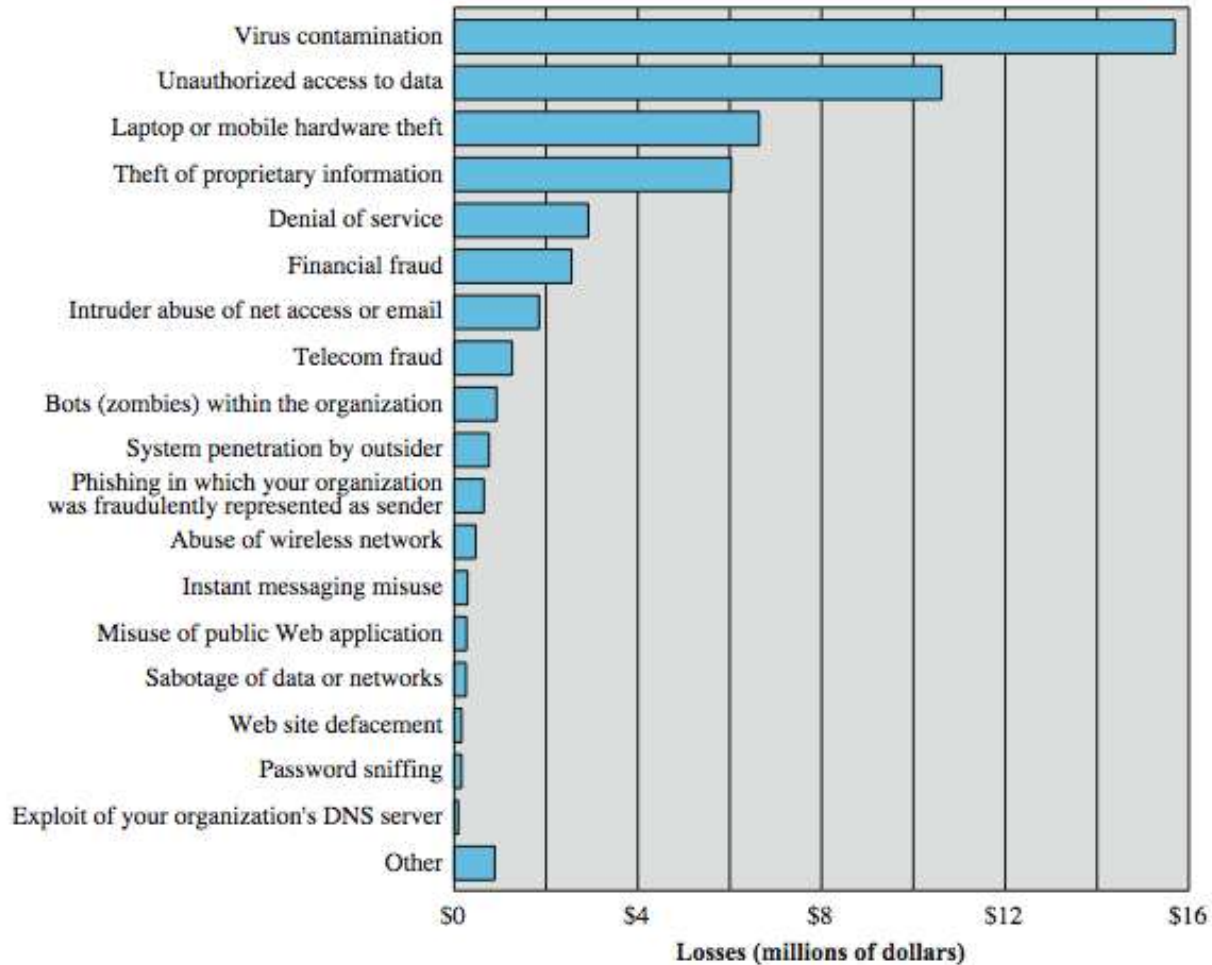
Security Taxonomy



Security Trends

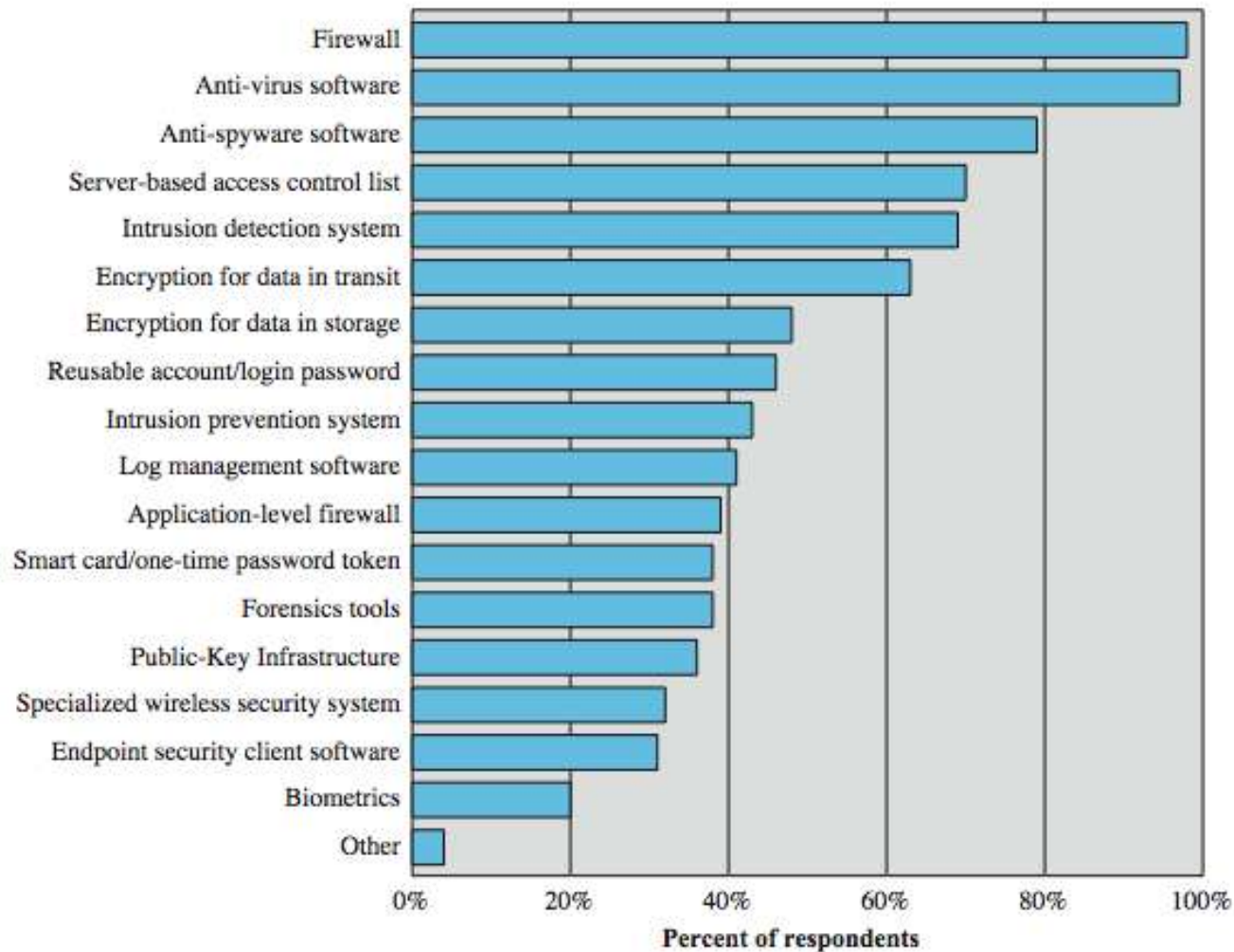


Computer Security Losses



Source: Computer Security Institute/FBI 2006 Computer Crime and Security Survey

Security Technologies Used



Source: Computer Security Institute/FBI 2006 Computer Crime and Security Survey

Security Technologies Used



- The popularity of certain tools reflects a number of factors:
 - **The maturity** of these technologies means that security administrators are *very familiar with the products* and are confident of their effectiveness.
 - Because these technologies are mature and there are a number of vendors, *costs tend to be quite reasonable* and user-friendly interfaces are available
 - The threats countered by these technologies are *among the most significant* facing security administrators.

Computer Security Strategy



- A comprehensive security strategy involves
 - **specification/policy** – what is the security scheme supposed to do?
 - **Implementation/mechanism** – How does it do it?
 - **Correctness/assurance** – Does it really work?

Computer Security Strategy



- **specification/policy**
 - A security policy is an informal description of desired system behavior.
 - In developing a security policy, a security manager needs to consider the context, in terms of:
 - ✦ value of the assets being protected;
 - ✦ vulnerabilities of the system;
 - ✦ potential threats and the likelihood of attacks.
 - Further, the manager must consider the following tradeoffs between
 - ✦ “Ease of use versus security” and
 - ✦ “Cost of security versus cost of failure and recovery”

Computer Security Strategy



- **implementation/mechanisms**
 - Security implementation involves four complementary courses of action:
 - ✦ prevention (when unauthorized access is critical, first line of defense),
 - ✦ detection (when practical to detect security attacks),
 - ✦ response (to halt the attack and prevent further damage),
 - ✦ recovery (from attack consequences, such as using a backup system).

Computer Security Strategy



- **correctness/assurance**
 - **Assurance** as the degree of confidence one has that the security measures, both technical and operational, work as intended to protect the system and the information it processes.
 - **Evaluation** is the process of examining a computer product or system with respect to certain criteria.
 - ✦ Evaluation involves testing, and may also involve formal analytic or mathematical techniques.

Summary



- security concepts
- terminology
- functional requirements
- security trends
- security strategy

Assignment 2



TITLE:

**CYBER ATTACK TRENDS AND WHERE
OUR FOCUS SHOULD BE.**

MARKS %: 3