Module 1: Terminologies

Dr. Natarajan Meghanathan
Associate Professor of Computer Science
Jackson State University, Jackson, MS 39217
E-mail: natarajan.meghanathan@jsums.edu

Introduction

- What is Computer Security?
  - Computer-related assets: the threats and counter measures to protect the assets

  - 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" (includes hardware, software, firmware, information/data, and telecommunications).

CIA Triad: Three Fundamental Concepts of Information Security

- **Confidentiality**
  - Data confidentiality: Assure that private or confidential info is not disclosed to ***unauthorized*** individuals.
  - Privacy: Individuals need to be able to control what information that is related to them is disclosed to others and to whom.

- **Integrity**
  - Data Integrity: Information and programs should be changed only in a specified and authorized manner.
  - System Integrity: A system should perform its function without any deliberate/unauthorized manipulation of the system.

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

Authentication and Accountability

- Authentication
  - Verifying that users are who they say they are and that each input arriving at the system are from a trusted source.

- Accountability
  - Actions on an entity should be uniquely traceable to that entity (to support non-repudiation, intrusion detection and prevention, fault isolation, forensics investigation and etc.)

Computer Security Terminology

- Asset (System Resource)
  - ***Hardware***: Computer systems and other data processing devices, data storage and data communication devices
  - ***Software***: OS, system utilities and applications
  - ***Data***: Files and databases as well as security-related data such as password files.
  - ***Communications facilities and networks***: Local and wide area networks, communication links, bridges, routers, etc.
- Security Policy
  - A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.
  - ***Factors to consider***: Value of the assets being protected; vulnerabilities of the system; Potential threats and the likelihood of attacks.
  - ***Tradeoffs to consider***: Ease of use vs. security; Cost of security vs. cost of failure and recovery.

Computer Security Terminology

- Vulnerability: A flaw or weakness in the system's design, implementation or operation that could be exploited

- Threat: A possible danger (circumstance, capability, action or event) that might exploit a vulnerability and cause harm.

- Risk: The chances (probability) that a particular threat will exploit a vulnerability

- Attack: The sequence of events that executes the threat on an asset.

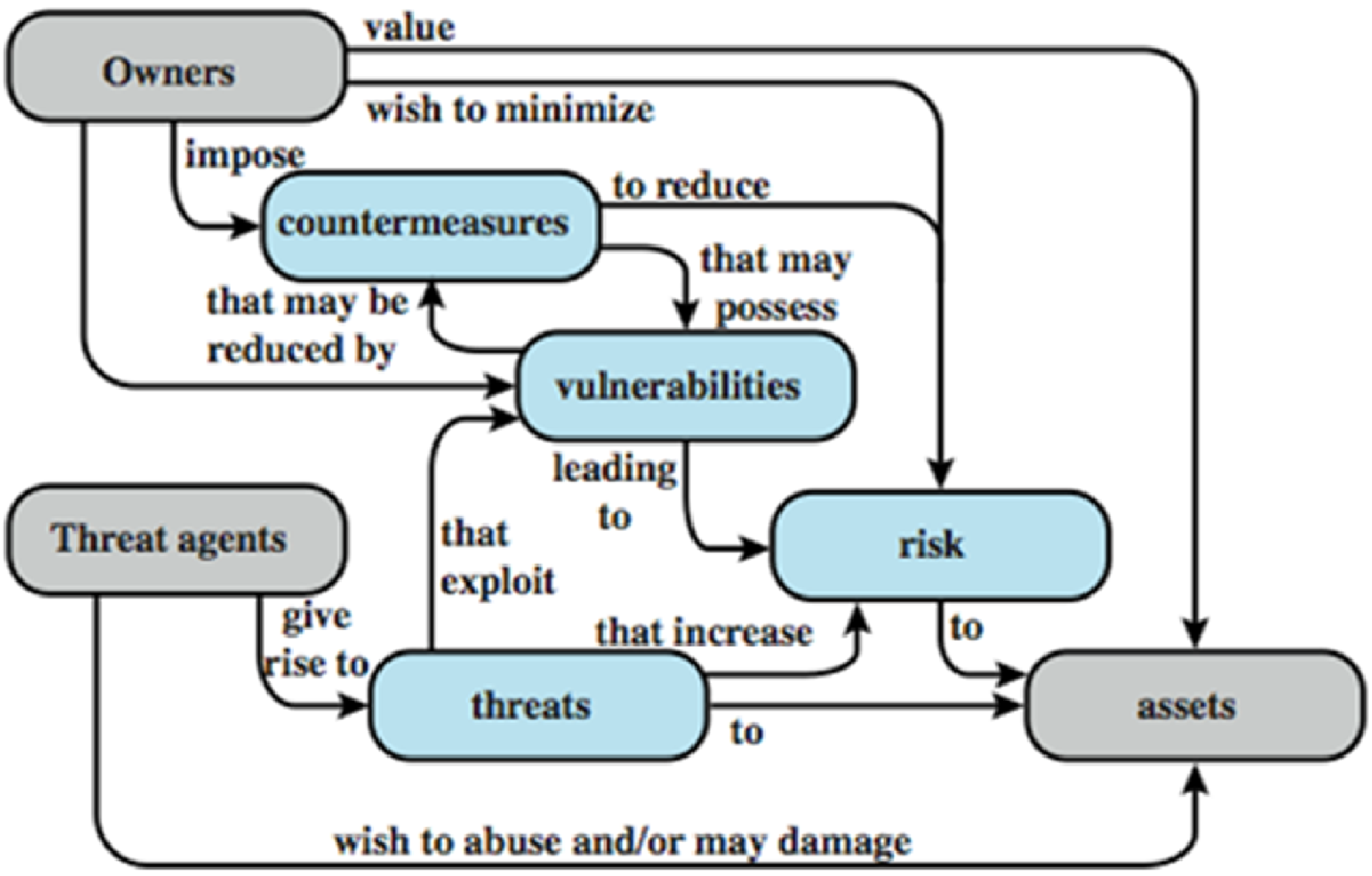
- Countermeasure: An action, device, procedure or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause.

- Adversary: An entity that attacks or is a threat to a system.

Vulnerabilities, Threats and Attacks

- **Vulnerability**
    - corrupted (loss of integrity)
    - leaky (loss of confidentiality)
    - unavailable or very slow (loss of availability)
- **Threat**
    - capable of exploiting vulnerabilities
    - represent potential security harm to an asset
- **Attacks**
    - Active attack (to cause harm); Passive attack (to learn or make use of system information, without causing any harm)
        - The focus is to detect active attacks and recover from their effects; Passive attacks (like Traffic Analysis) can be typically only prevented (using schemes like Encryption).
    - Inside attack (insider – one who is authorized to access system resources; but accesses them in a way not approved by those who granted the authorization); Outside attack (initiated from outside – unauthorized users)

Security Concepts and Relationships

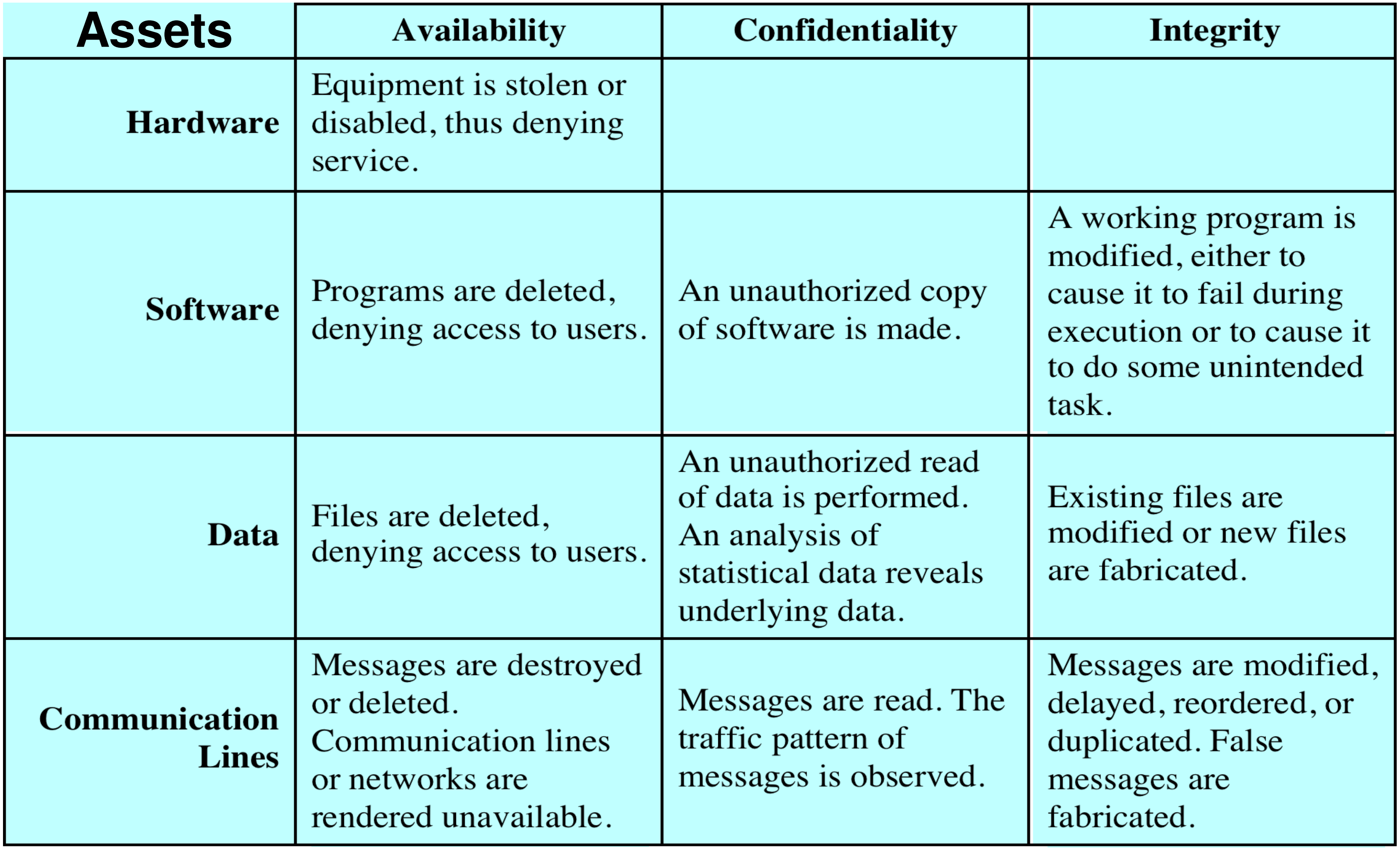


Source: Figure 1.2; W. Stallings, Computer Security: Principles and Practice, 2nd Edition

Threat Consequence	Threat Action (attack)
Unauthorized Disclosure A circumstance or event whereby an entity gains access to data for which the entity is not authorized. **(Confidentiality)**	**Exposure:** Sensitive data are directly released to an unauthorized entity. **Interception:** An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. **Inference:** A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or byproducts of communications. **Intrusion:** An unauthorized entity gains access to sensitive data by circumventing a system's security protections.
Deception **(Integrity)** A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.	**Masquerade:** An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. **Falsification:** False data deceive an authorized entity. **Repudiation:** An entity deceives another by falsely denying responsibility for an act.
Disruption **(Availability)** A circumstance or event that interrupts or prevents the correct operation of system services and functions.	**Incapacitation:** Prevents or interrupts system operation by disabling a system component. **Corruption:** Undesirably alters system operation by adversely modifying system functions or data. **Obstruction:** A threat action that interrupts delivery of system services by hindering system operation.

Source: Table 1.2; W. Stallings, Computer Security: Principles and Practice, 2nd Edition

Computer and Network Assets, with Examples of Threats

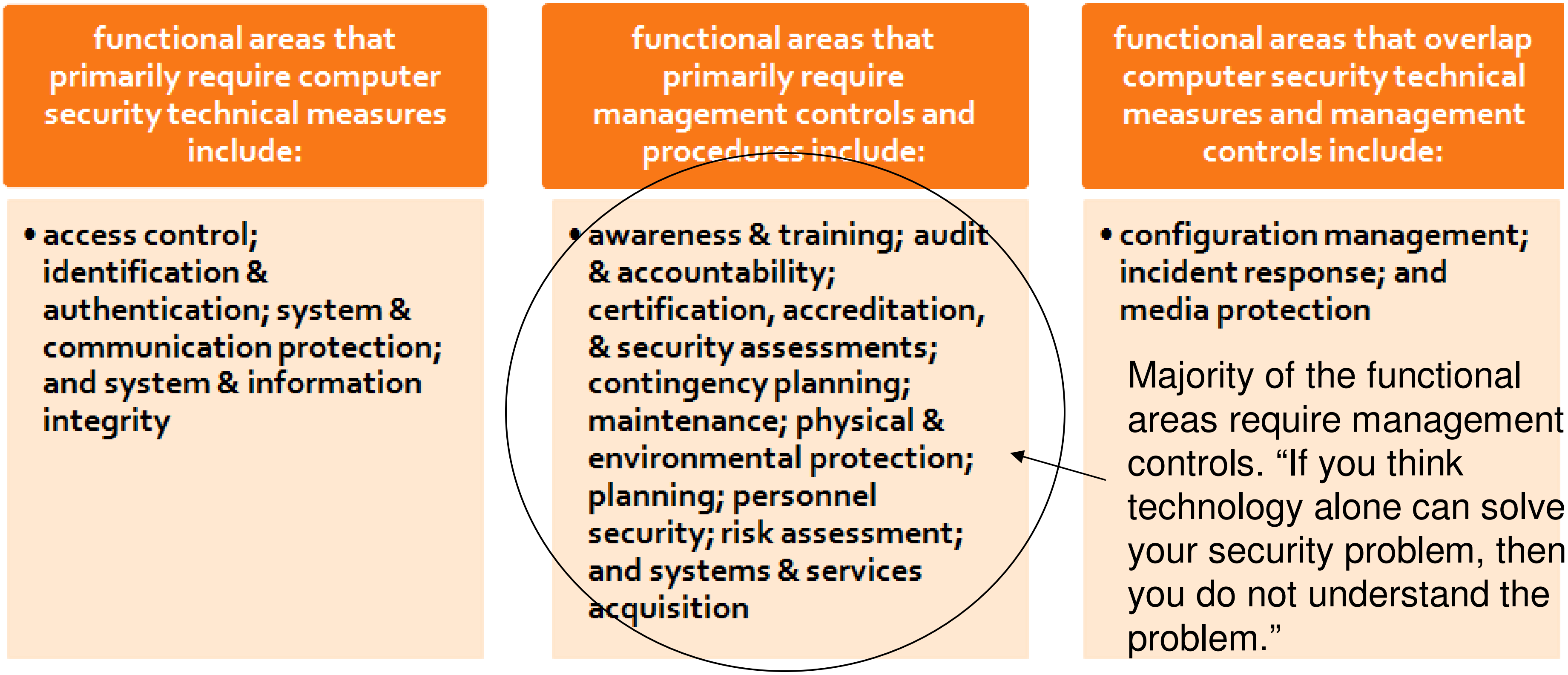


Assets	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.		
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to 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	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.

Source: Table 1.3; W. Stallings, Computer Security: Principles and Practice, 2nd Edition

Countermeasures

- Countermeasures could be viewed as functional requirements of a system.
- Countermeasures could be classified based on those that require computer security technical measures (hardware/ software or both); managerial issues; or both.



functional areas that primarily require computer security technical measures include:	functional areas that primarily require management controls and procedures include:	functional areas that overlap computer security technical measures and management controls include:
• access control; identification & authentication; system & communication protection; and system & information integrity	• awareness & training; audit & accountability; certification, accreditation, & security assessments; contingency planning; maintenance; physical & environmental protection; planning; personnel security; risk assessment; and systems & services acquisition	• configuration management; incident response; and media protection

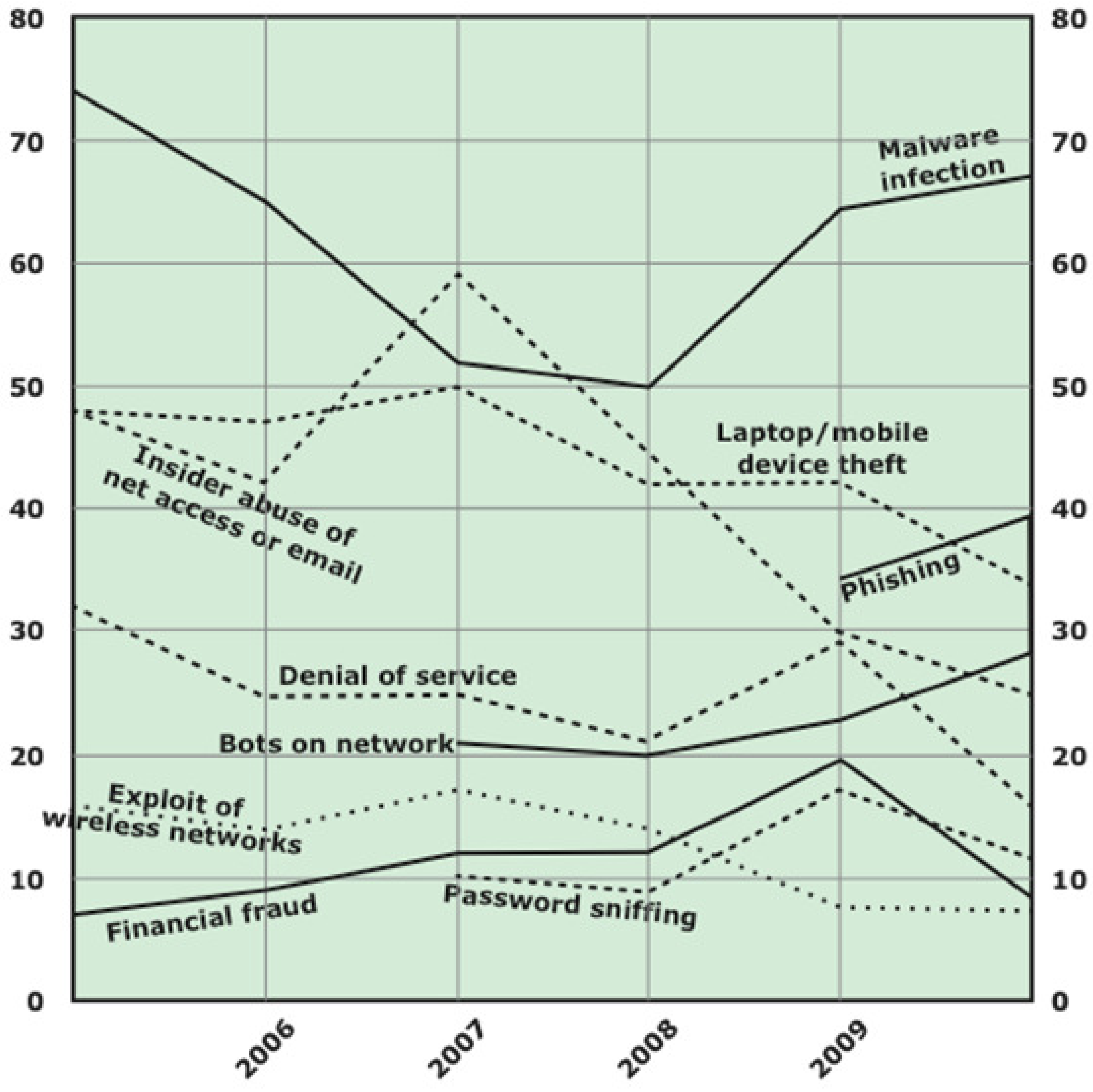
Majority of the functional areas require management controls. “If you think technology alone can solve your security problem, then you do not understand the problem.”

Security Mechanism vs. Security Service

- **Security Mechanism:** A mechanism that is designed to detect, prevent or recover from a security attack.
  - **Examples:** Encryption, Digital signature, Routing control, Traffic padding, Notarization

- **Security Service:** A service that enhances the security of the data processing systems and the information transfers of an organization.
- The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.
  - **Examples:** Authentication, Access control, Data confidentiality, Data integrity, Non-repudiation, Availability

Security Trends

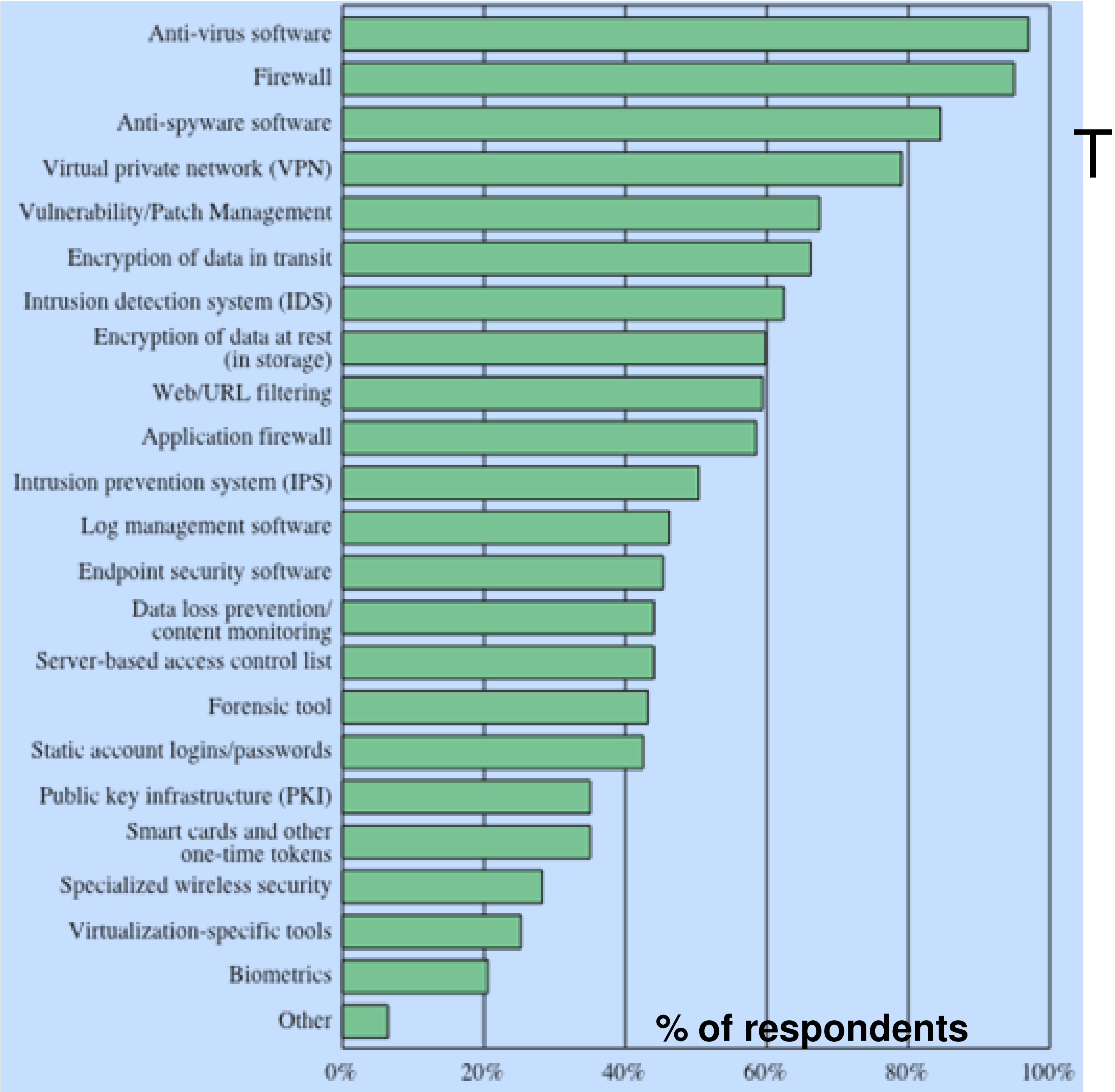


Attacks Experienced

(Source:
Computer Security
Institute 2010/2011
Computer Crime
and Security Survey)

% of respondents

Security Technologies Used



(Source:
Computer Security
Institute 2010/2011
Computer Crime
and Security Survey)