Information Security

Chapter 1: Overview

Nguyễn Đăng Quang

Chapter 1: Overview

- Computer Security Concepts and Terminology
- Fundamental Security Design Principles
- Attack Surfaces and Attack Trees
- Information Security Strategy

Learning objectives

- Describe the key security requirements of confidentiality, integrity and availability
- Discuss the types security threats and attacks
- Explain the fundamental security design principles
- Discuss the use of attack surfaces and attack trees
- Understand the principle aspects of a comprehensive security strategy

A Definition of Computer Security

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).

NIST

Three Key Objectives (the CIA triad)

1. **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.

Three Key Objectives (the CIA triad)

2. **Integrity**

   Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.

   A loss of integrity is the unauthorized modification or destruction of information.

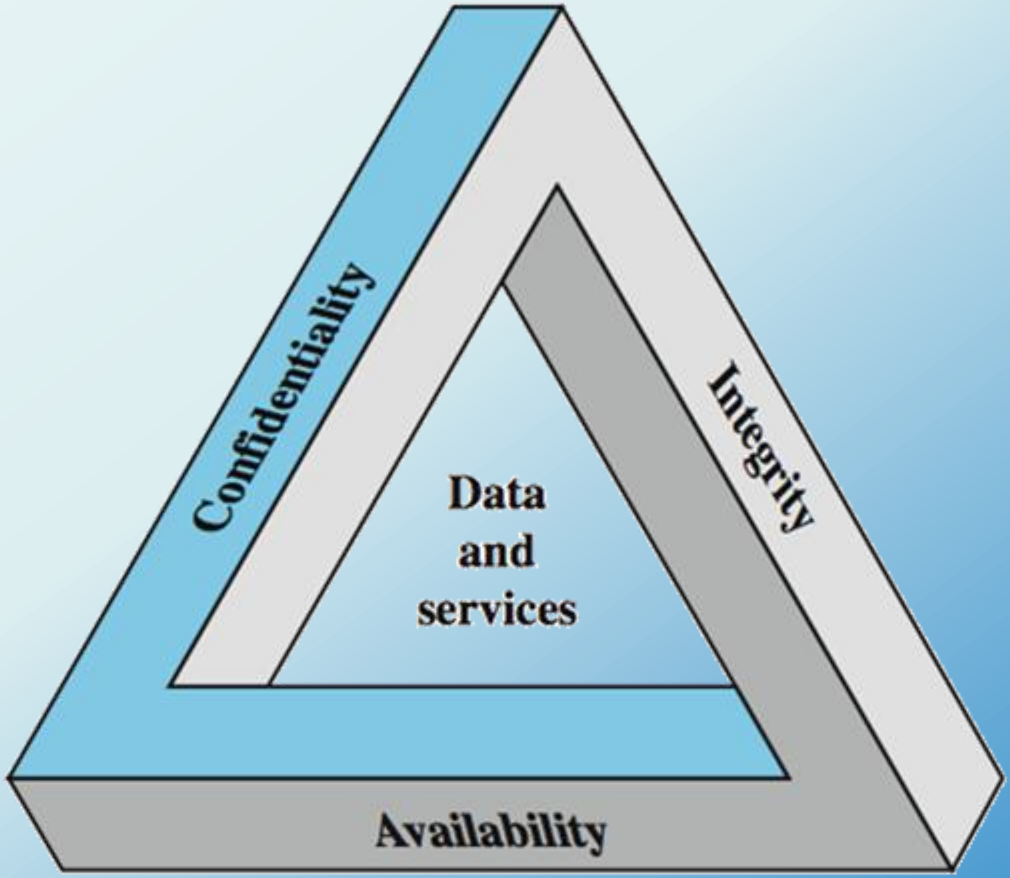
Three Key Objectives (the CIA triad)

3. **Availability**:

   Assure that systems works promptly, and service is not denied to authorized users.

   A loss of availability is the disruption of access to or use of information or an information system.

Key Security Concepts



A Complete Security Picture

- **Authenticity**:

  the property of being genuine and being able to be verified and trusted; confident in the validity of a transmission, or a message, or its originator

- **Accountability**:

  generates the requirement for actions of an entity to be traced uniquely to that individual to support nonrepudiation, deference, fault isolation, etc.

Challenges of Computer Security

1. Computer security is not simple.
2. One must consider potential (unexpected) attacks.
3. Procedures used are often counter-intuitive.
4. Must decide where to deploy mechanisms.
5. Involve algorithms and secret info (keys).
6. A battle of wits between attacker / admin.
7. It is not perceived on benefit until fails.
8. Requires constant monitoring.
9. Too often an after-thought (not integral).
10. Regarded as impediment to using system.

Computer Security Terminology

- Vulnerability
- Threat
- Adversary (Threat Agent or Threat Actor)
- Asset
- Attack
- Countermeasure
- Risk
- Security Policy

Fundamental Security Design Principles

(Saltzer and Schroeder's design principles)

- Despite years of research, it is still difficult to design systems that comprehensively prevent security flaws
- But good practices for good design have been documented (analogous to software engineering)
- Simplicity, Fail-Safe defaults, Complete Mediation, Open Design, No single point-of-failure, Minimum Exposure, Separation of Privileges, Least Privilege, Maximize the Entropy of Secrets, Traceability, Usability.

Fundamental Security Design Principles

1. **Economy of mechanism** (Simplicity)
2. **Fail-safe default**
3. **Complete mediation**: every access should be checked against an access control system
4. **Open design**: the design should be open rather than secret (e.g., encryption algorithms)
5. **No single-point-of-failure** (separation of privilege)

Fundamental Security Design Principles

6. **Compartmentalization:** organize resource into isolated groups similar needs.
7. **Minimum exposure:** minimize the attack surface a system presents to the adversary.
8. **Separation of privilege**: multiple privileges should be needed to do achieve access (or complete a task)
9. **Least privilege**: every user (process) should have the least privilege to perform a task
10. Maximize the entropy of secrets

Fundamental Security Design Principles

11. **Traceability**: Log security-relevant system events
12. **Psychological Acceptablility**: security mechanisms should not make the resource more difficult to access than without it.

Attack surfaces

- Attack surface: the reachable and exploitable vulnerabilities in a system
  - Open ports
  - Services outside a firewall
  - An employee with access to sensitive info

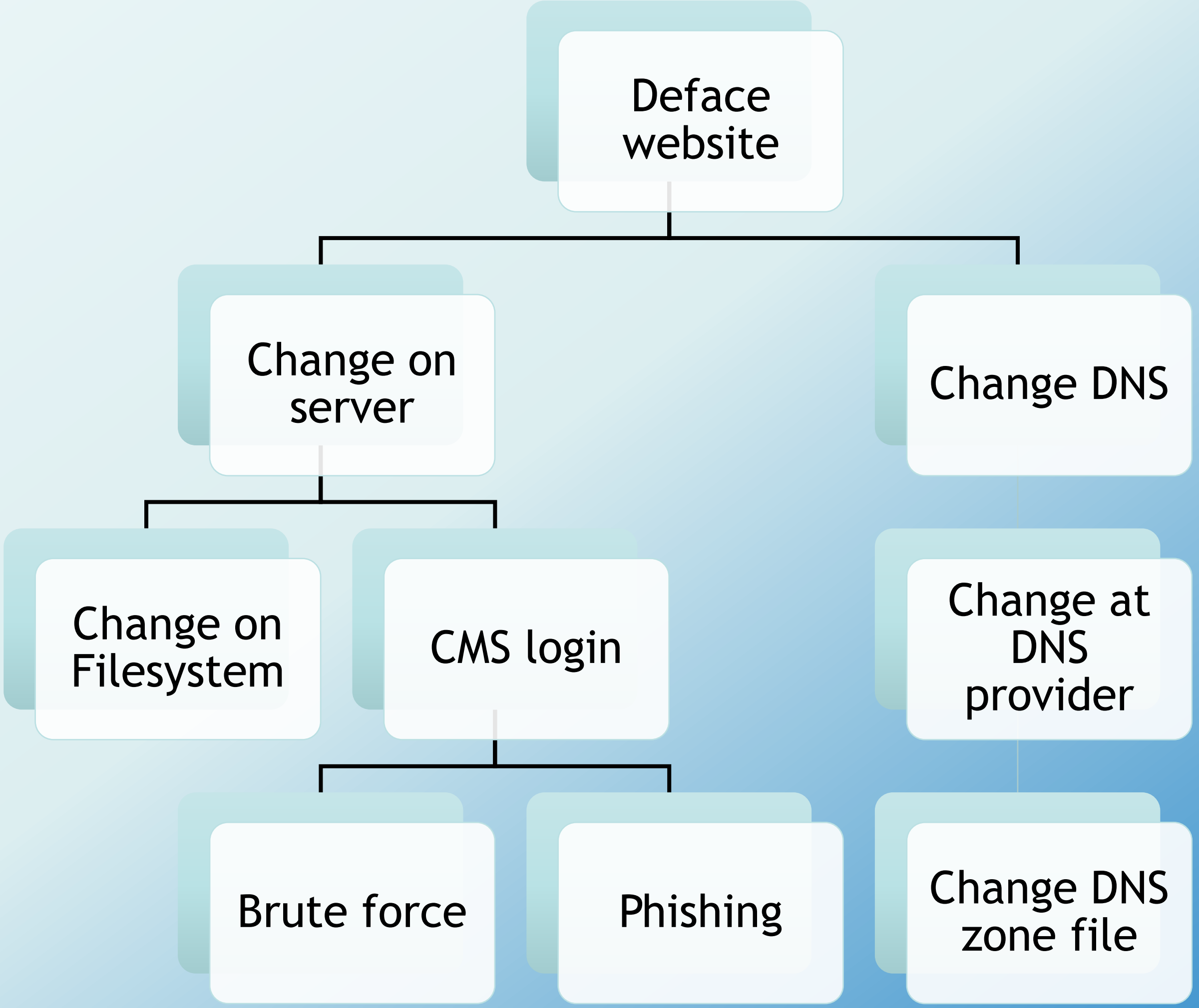
Attack surfaces

- Categories
  - **Network attack surface** (i.e., network vulnerability)
  - **Software attack surface** (i.e., software vulnerabilities)
  - **Human attack surface** (e.g., social engineering)
- Attack analysis: assessing the scale and severity of threats

Attack trees

- A branching, hierarchical data structure that represents a set of potential vulnerabilities
- Objective: to effectively exploit the info available on attack patterns
  - Security analysts can use the tree to guide design and strengthen countermeasures

Attack Tree


Deface website

Change on server

Change DNS

Change on Filesystem

CMS login

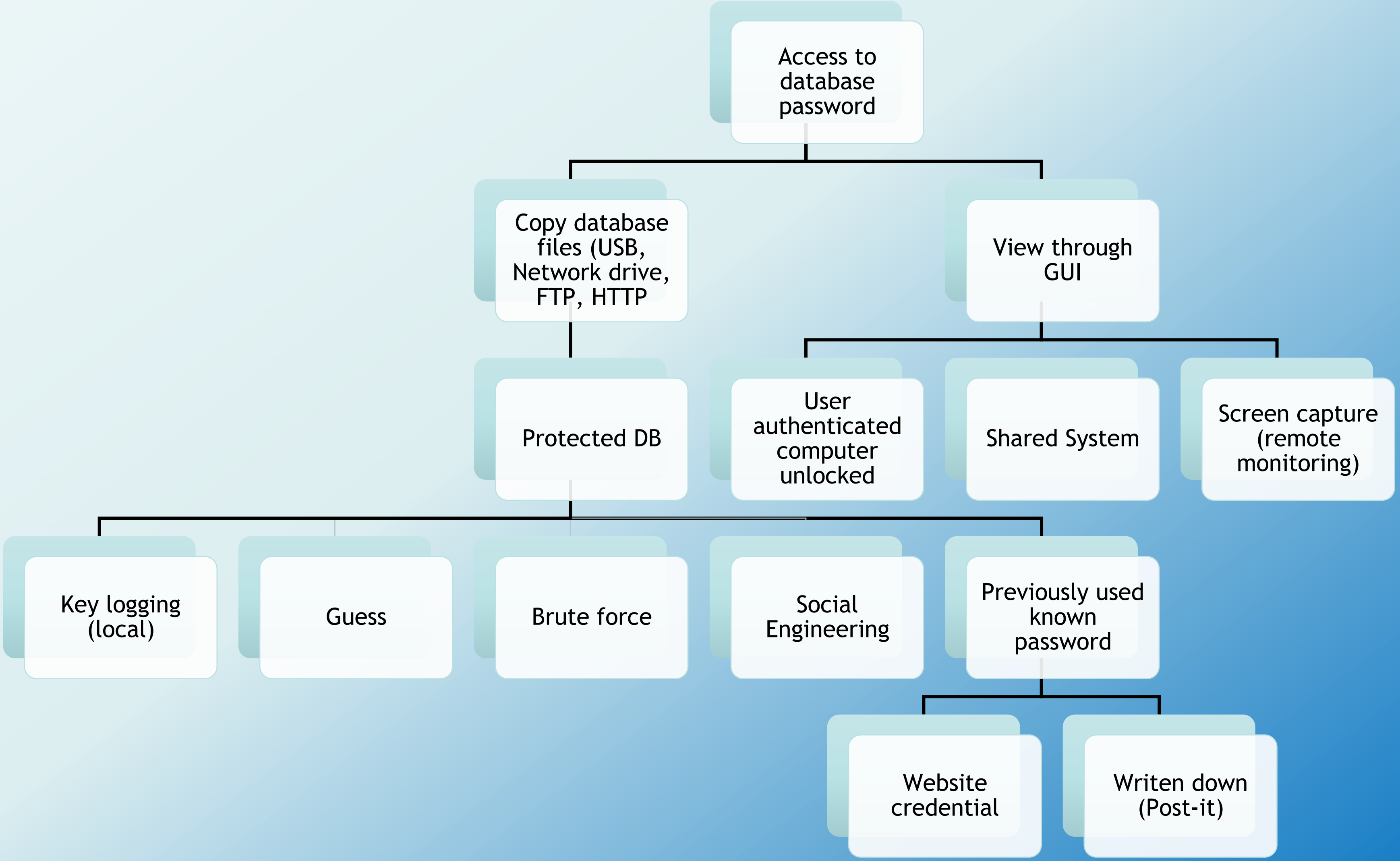
Change at DNS provider

Brute force

Phishing

Change DNS zone file

Attack Tree

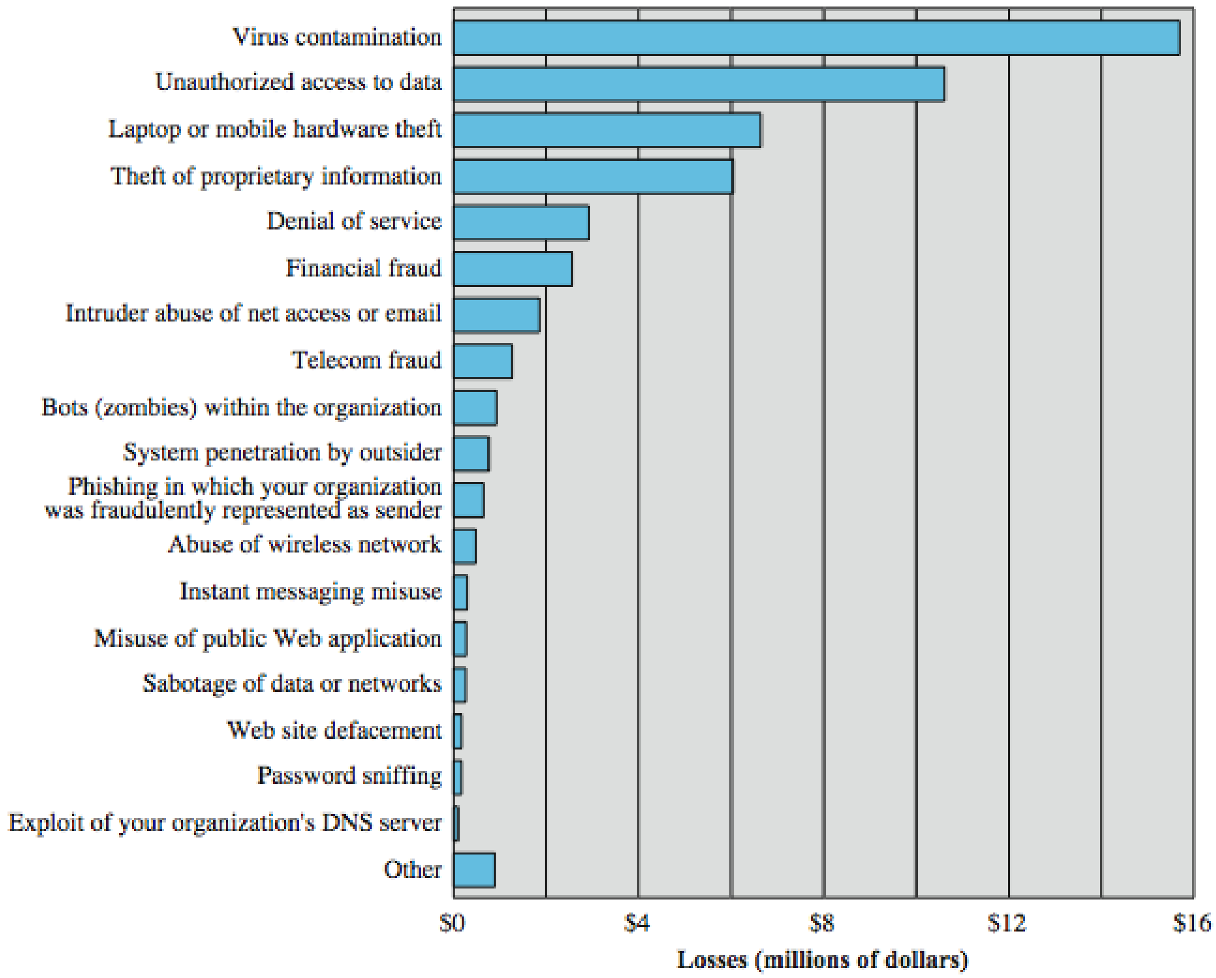

Access to database password
Copy database files (USB, Network drive, FTP, HTTP
View through GUI
Protected DB
User authenticated computer unlocked
Shared System
Screen capture (remote monitoring)
Key logging (local)
Guess
Brute force
Social Engineering
Previously used known password
Website credential
Writen down (Post-it)

Information Security Strategy

An overall strategy for providing security

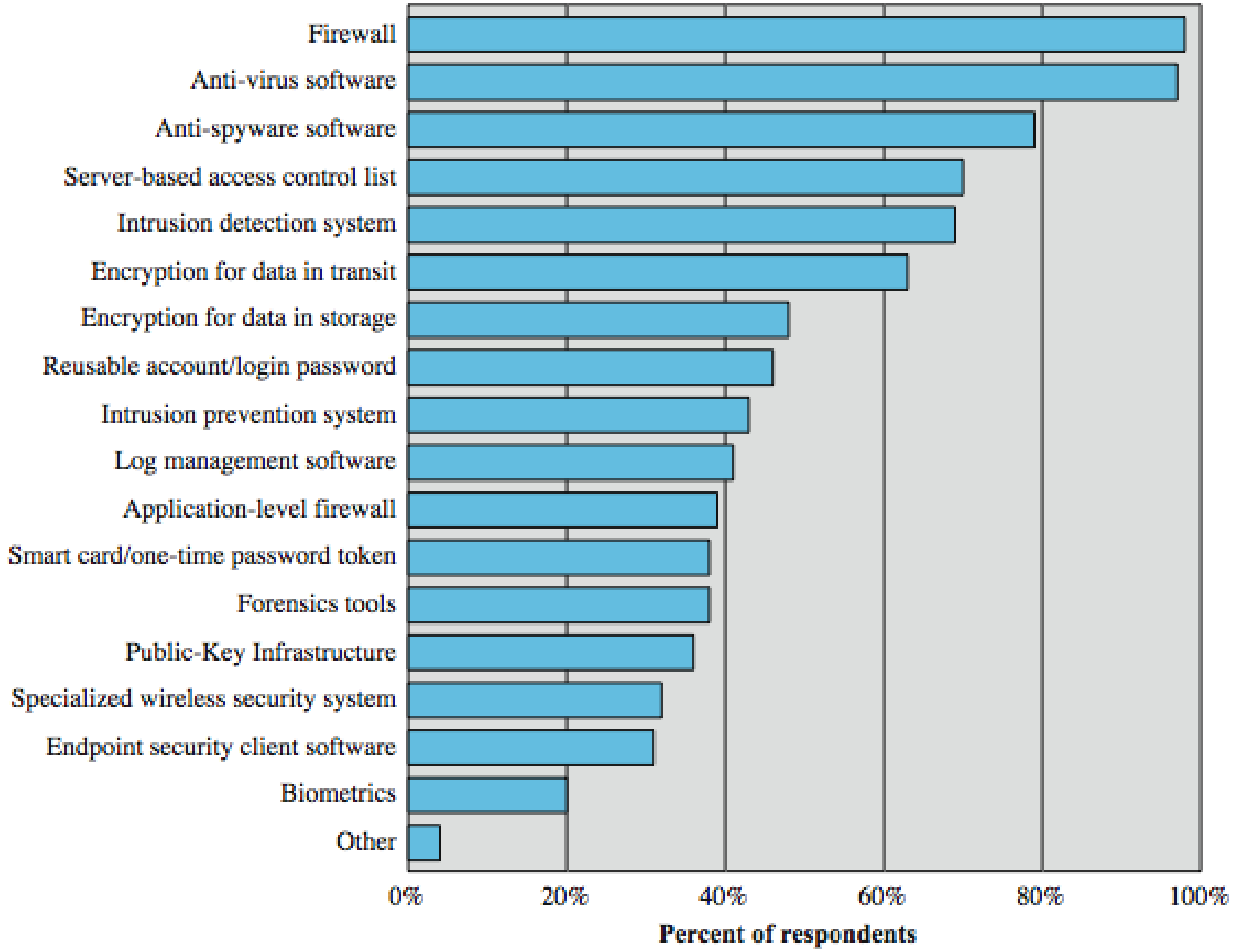
- **Policy** (specs): what security schemes are supposed to do
  - Assets and their values
  - Potential threats
  - Ease of use vs security
  - Cost of security vs cost of failure/recovery
- **Implementation/mechanism**: how to enforce
  - Prevention
  - Detection
  - Response
  - Recovery
- **Correctness/assurance**: does it really work (validation/review)

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

Summary

- Security concepts
- Terminology
- Security design principles
- Attack surface & Attack Tree
- Security strategy