CYBR3000

Cybersecurity Overview

Dr Dan Kim

Associate Professor in Cybersecurity,
School of EECS
The University of Queensland, Australia
Homepage: https://researchers.uq.edu.au/researcher/23703

Learning objectives

- At the end of this lecture, you will be able to Understand/explain
  - Computer Security Concepts
  - Threats, Attacks, and Assets
  - Security Functional Requirements
  - Fundamental Security Design Principles
  - Attack Surfaces and Attack Trees
  - Computer Security Strategy

Computer Security definition?

- 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).

*National Institute of Standards and Technology

Three key objectives (the CIA triad)

- **C**onfidentiality
  - preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
- **I**ntegrity
  - guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity
- **A**vailability
  - ensuring timely and reliable access to and use of information

https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html

Security objectives (cont.)

An example

Internet

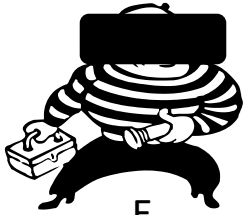
Alice in Brisbane

UGETGV

Bob in Sydney

by modern ciphers DES, 3DES, AES, *etc*

by a Classical Cipher named Caesar with *k=2*



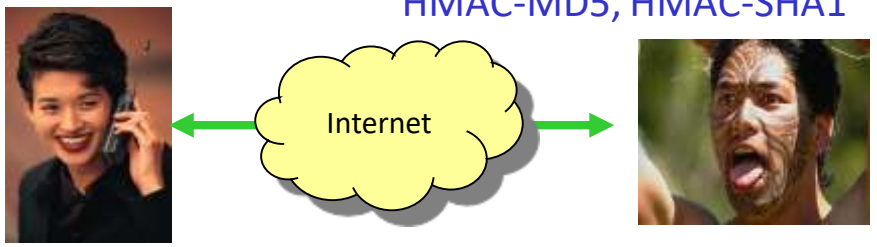
E

The data has not been viewed by a 3rd party → ***C****onfidentiality* ← Encryption

C*onfidentiality: the protection of transmitted data from passive attacks (release of message contents and traffic analysis)*

Security objectives (cont.)

Use Hashed message authentication code (HMAC), such as HMAC-MD5, HMAC-SHA1



Alice in Brisbane

Bob in Sydney

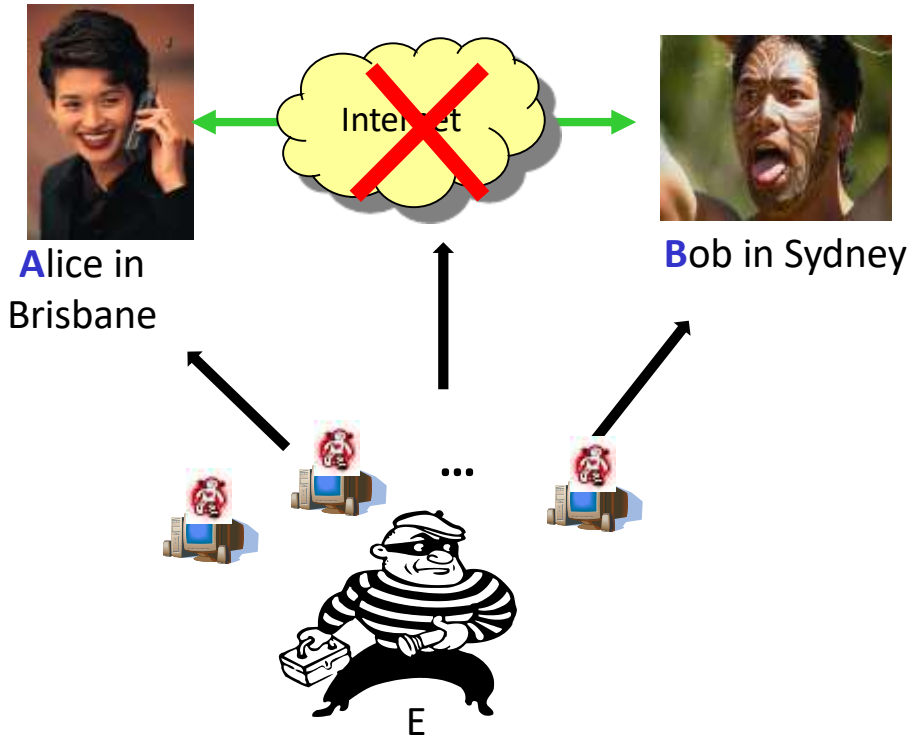
Unclassified code3000
- I hate you!

E

The data has not been modified in transit → ***I****ntegrity* ← Crytographic Hash func.

I*ntegrity: the assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay)*

Security objectives (cont.)



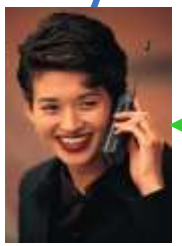
Distributed Denial of Service (DDoS) attacks

For any information system to serve its purpose, the information must be **available** when it is needed

→ **A**vailability

Source: http://memeburn.com

Security objectives : summary



Internet

Alice in Brisbane

Bob in Sydney

Cryptography

The data has not been viewed by a 3rd party → ***C**onfidentiality* ← Encryption

The data has not been modified in transit → ***I**ntegrity* ← Hash func.

The data must be **available** when it is needed → **A**vailability

Additional Security Goals

- Authenticity:
  - The property of being genuine and being able to be verified and trusted
  - This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
  - FIPS* PUB 199 (i.e., NIST standards for security categorization) includes authenticity under integrity.

- Accountability:
  - The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
  - This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
  - truly secure systems aren't yet an achievable goal, we must be able to trace a security breach to a responsible party.

*The Federal Information Processing Standards **Publication** Series of the National Institute of. Standards and Technology (NIST)
Web: https://csrc.nist.gov/publications/detail/fips/199/final

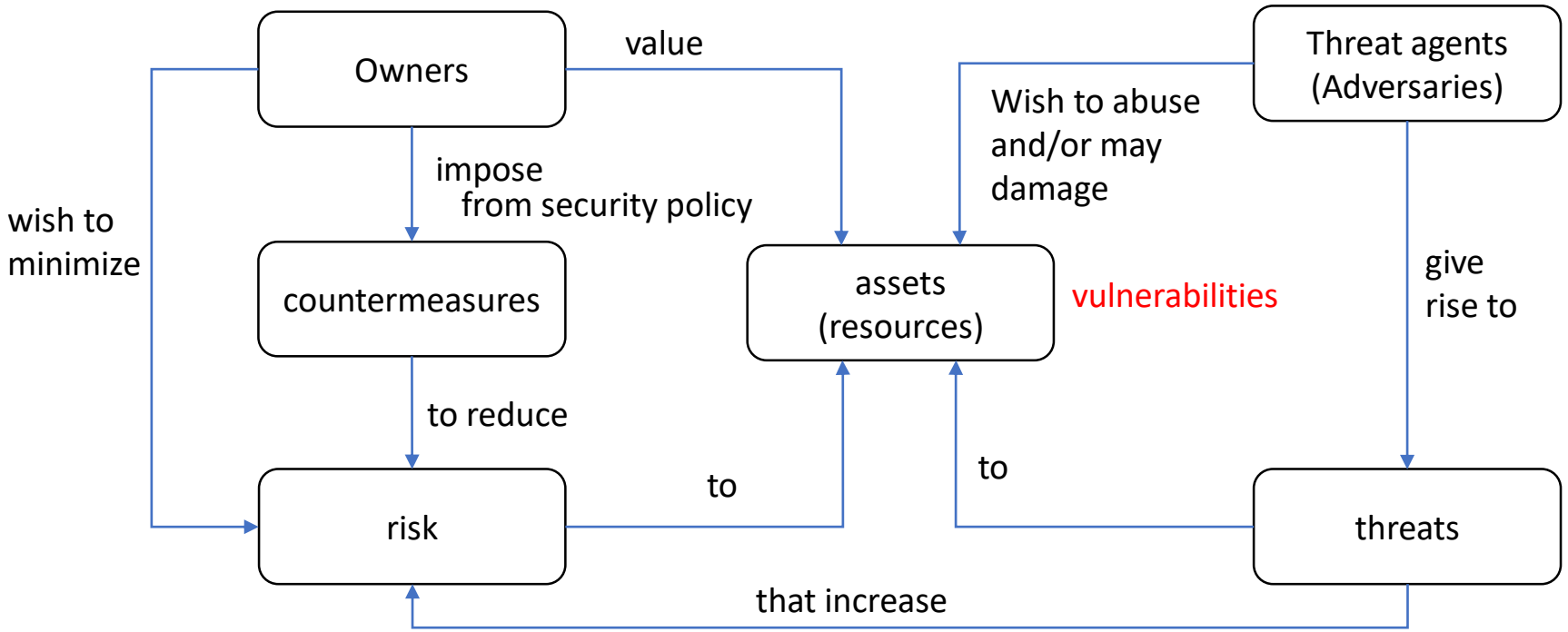
University example?

- Confidentiality
  - Student login password should not be improperly disclosed by others
  - e.g., ID: abc123 password: p@ssw0rd!
  - Q: any other examples?

- Integrity
  - Student name should not be modified improperly
  - e.g., John -> Jonathan
  - Q: any other examples?

- Availability
  - **Learn** (blackboard) system should be available when a student wants to download lecture slides.
  - Q: any other examples?

Security concepts and Relationships



Explain this!

Computer Security Terminology

- System Resource (Asset)
  - Data contained in an information system;
  - or a service provided by a system;
  - or system capability, such as processing power or communication bandwidth;
  - or an item of system equipment (i.e., a system component – hardware, firmware, software, or documentation);
  - or a facility that houses system operations and equipment
- Vulnerability
  - A 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 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

Request for Comments (RFC) 4949, Internet Security Glossary, May 2000

Computer Security Terminology (cont.)

- Adversary (Threat agent)
  - An entity that attacks, or is a threat to, a system
- 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; That is, a threat is a possible danger that might exploit a vulnerability
- Attack
  - An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system

Computer Security Terminology (cont.)

- Intrusion:
  - an attack that succeeds (or all the activities of violation of C.I.A in IDS)
- 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.

Attacks and their classifications

Alter?

- Passive:
  - attempt to learn or make use of information from the system that does not affect system resources; eavesdropping on, or monitoring of, transmissions;
  - Two types: release of message contents; traffic analysis
- Active
  - attempt to alter system resources or affect their operation
  - Four categories: Replay, Masquerade, Modification of messages, Denial of service

Origin?

- Inside
  - initiated by an entity inside the security perimeter
- Outside
  - initiated from outside the perimeter

Countermeasure to Security Vulnerabilities and Threats

in terms of Security Requirements

(FIPS PUB 200)

*Minimum Security Requirements for Federal Information Processing Standards Publications (17 security-related areas w.r.t. protecting C.I.A.)

- 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 (both digital & paper)

Attack Surfaces

- consists of the reachable and exploitable vulnerabilities in a system
- Examples
  - Open ports on outward facing Web and other servers, and code listening on those ports
  - Services available on the inside of a firewall
  - Code that processes incoming data, email, XML, office documents, and industry-specific custom data exchange formats Interfaces, SQL, and Web forms
  - **An employee** with access to sensitive information vulnerable to a social engineering attack

Attack Surfaces: categories

Network Attack Surface

Vulnerabilities over an enterprise network, wide-area network, or the Internet

Included in this category are network protocol vulnerabilities, such as those used for a denial-of-service attack, disruption of communications links, and various forms of intruder attacks

Software Attack Surface

Vulnerabilities in application, utility, or operating system code.

Particular focus is (Web) server software

Human Attack Surface

Vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders.

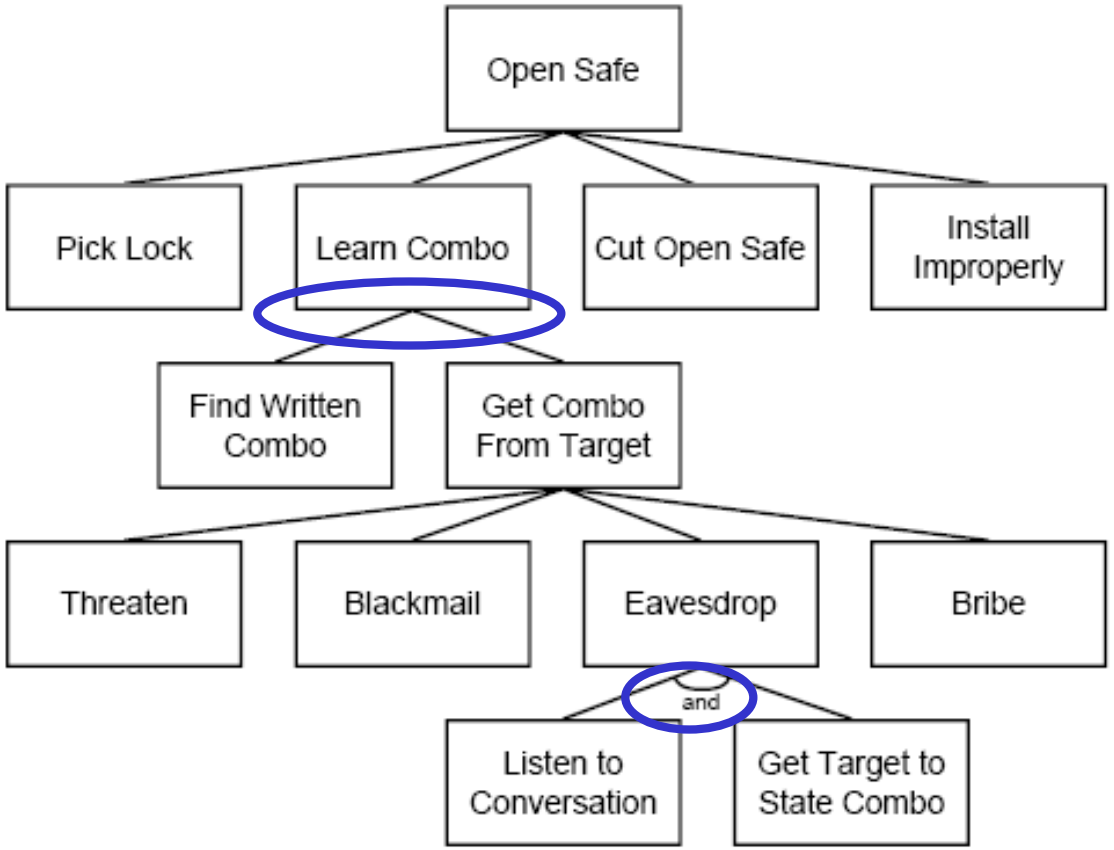
Attack trees

- A branching, hierarchical data structure that represents a set of potential vulnerabilities (events)

- Objective: to effectively exploit the info available on attack patterns
  - published on the US CERT* or similar forums
  - Security analysts can use the tree to guide design and strengthen countermeasures

*Cyber Emergency Response Team; aka, Computer Emergency Response Team (CERT) in the past.

An Attack Tree for “open safe”



Source: B. Schneier, https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Fundamental Security Design Principles to guide the development of protection mechanisms

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability
- Isolation
- Encapsulation
- Modularity
- Layering
- Least astonishment

Fundamental Security Design Principles

- Economy of Mechanism
  - Security mechanism should be as simple as possible.
    - ✓ A simple design is easier to test and validate. (kids can play with smartphone)
    - ✓ Fewer vulnerabilities
- Fail-Safe Defaults
  - Systems should default to a secure state, denying access by default and granting access only when explicit permission is given.
  - Most file access permissions work this way;
    - ✓ Windows access control list (ACL), Linux/Unix permissions
    - ✓ Firewalls (in the FW figure later)
- Complete mediation
  - Every access to every resource should be checked to ensure it is allowed.
    - ✓ the operating system checks the user requesting access against the file's ACL.
- Open design
  - Security of a mechanism should not depend upon secrecy of its design or implementation.
  - Should be open for scrutiny (critical observation or examination) by the community
  - Cryptography and openness
    - ✓ secure systems, including cryptographic systems, should have unclassified designs; eg. AES

Fundamental Security Design Principles

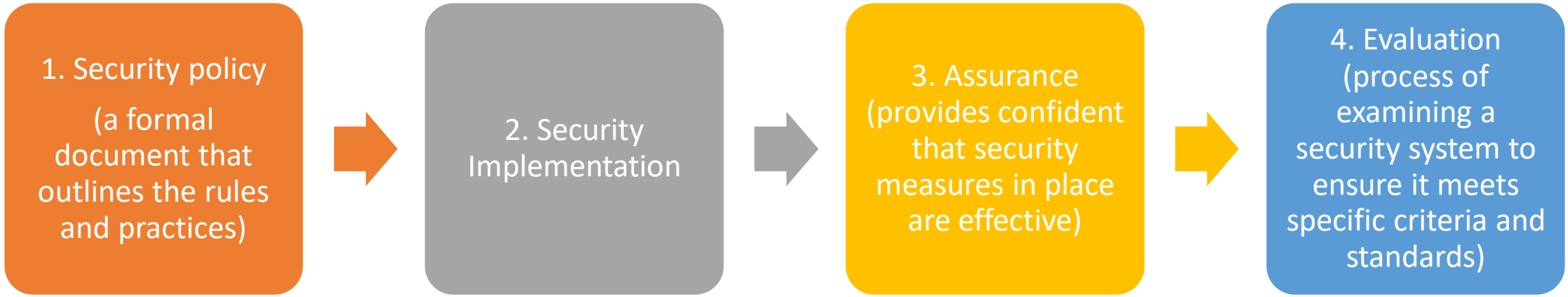
- Separation of privilege
  - System should not grant permission based on single condition; Access should be based on multiple conditions or credentials
    - ✓ Access to objects should depend on more than one condition being satisfied
    - ✓ e.g., Company checks over $75,000 to be signed by two officers.
    - ✓ e.g., dual keys for safety deposit boxes and the two-person control applied to nuclear weapons and top secret crypto materials.
- Least privilege
  - Entity (users and systems) should be given only those privilege needed to finish a task
    - ✓ Every program and user should operate while invoking as few privileges as possible.
    - ✓ This is the rationale behind Unix “sudo” and Windows User Account Control, both of which allow a user to apply administrative rights temporarily to perform a privileged task.
- Least Common Mechanism:
  - Mechanisms used to access resources should be minimized to avoid sharing that might lead to vulnerabilities.
- Psychological acceptability
  - the idea that the security mechanisms of a computer system should align as closely as possible to the functional expectations of system users.
  - By providing security mechanisms that do not burden or inconvenience users, architects can achieve security without alienation users or encouraging them to find ways to avoid security mechanisms.

Fundamental Security Design Principles

- Isolation
  - Public access should be isolated from critical resources (no connection between public and critical information) (e.g., net separation for critical infrastructure)
  - e.g., Users files should be isolated from one another (except when desired)
  - Security mechanism should be isolated (i.e., preventing access to those mechanisms) (FW, IDS, access control could be targets of attacks)
- Encapsulation
  - A design principle that separates the internal workings of a component from its external interface, improving modularity and security.
- Modularity
  - Systems should be composed of separate, self-contained components that can be independently developed, tested, and replaced.
- Layering (defense in depth):
  - The use of multiple layers of security controls to protect resources, ensuring that the failure of one control does not lead to a complete compromise.
- Least astonishment
  - a program or interface should always respond in a way that is least likely to astonish a user

Computer Security Strategy

to devise security services and mechanisms (simple view)



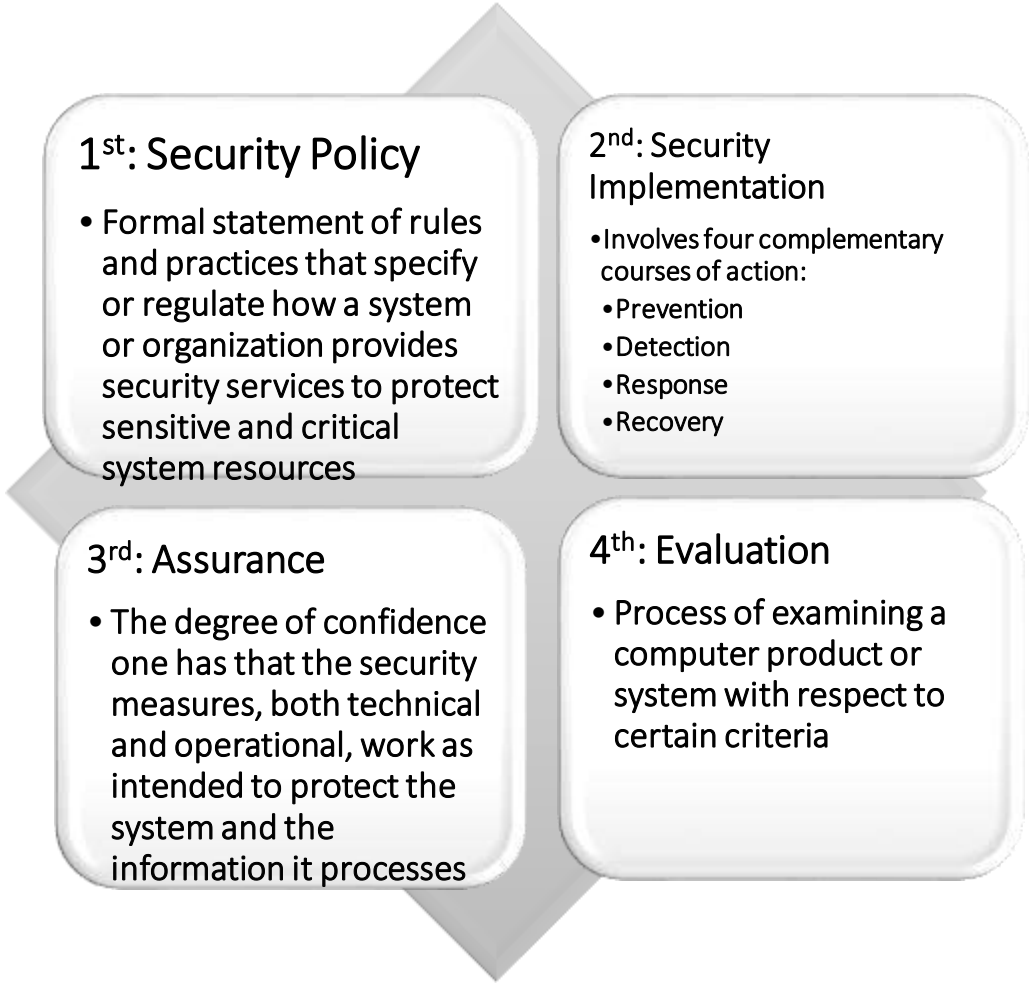
Computer Security Strategy

to devise security services and mechanisms (textbook version)

A security manager needs to consider the following factors:

- The value of the assets being protected
- The vulnerabilities of the system
- Potential threats and the likelihood of attacks

Assurance deals with the questions, “Does the security system design meet its requirements?” and “Does the security system implementation meet its specifications?”



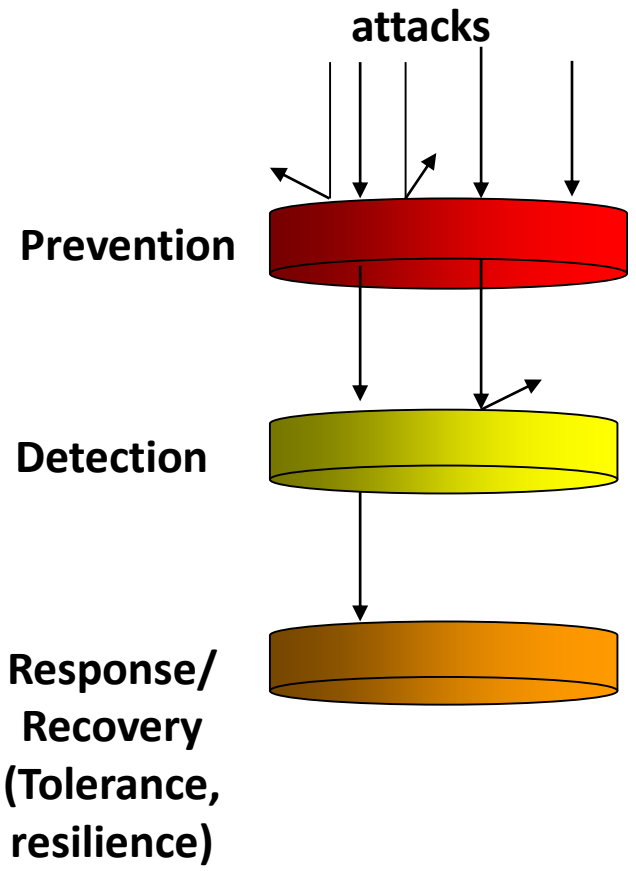
An ideal security scheme is one in which no attack is successful Absolute protection is not feasible, but it is practical to detect security attacks

If security mechanisms detect an ongoing attack, the system may be able to respond in such a way as to halt the attack and prevent further damage.

Evaluation involves testing and may also involve formal analytic or mathematical techniques.

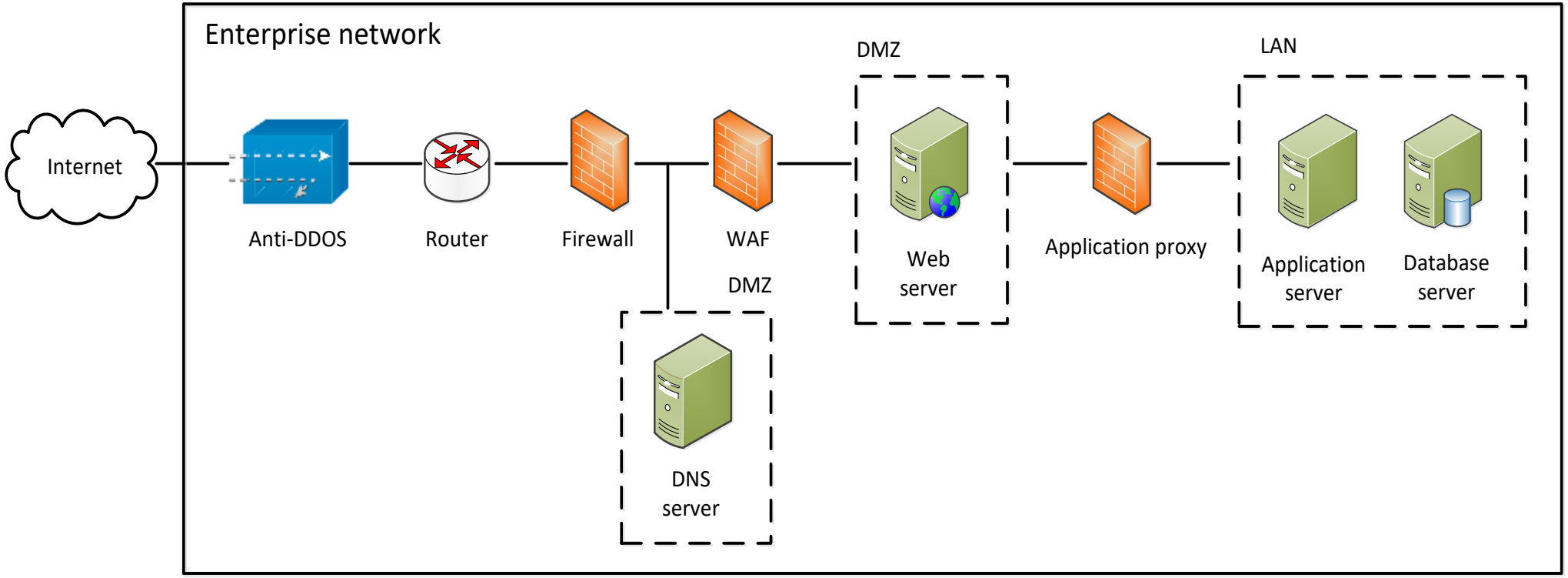
Security mechanisms/implementation

- Prevention
  - ✓ Example: encryption to prevent unauthorized access to data, access control (e.g., firewall, password/fingerprint)
- Detection
  - ✓ Example: Auditing and intrusion detection (e.g., Intrusion Detection System, forensics)
- Response
  - ✓ Example: halt the detected attack and prevent further damage
- Recovery
  - ✓ Data backup and reload correct copy of data
  - ✓ intrusion tolerance (e.g., Intrusion Tolerance System), backup



Q: What prevention, detection, response and recovery mechanism(s) can be used against a specific attack (e.g., DDoS attacks, Ransomware)?

An example of security mechanisms

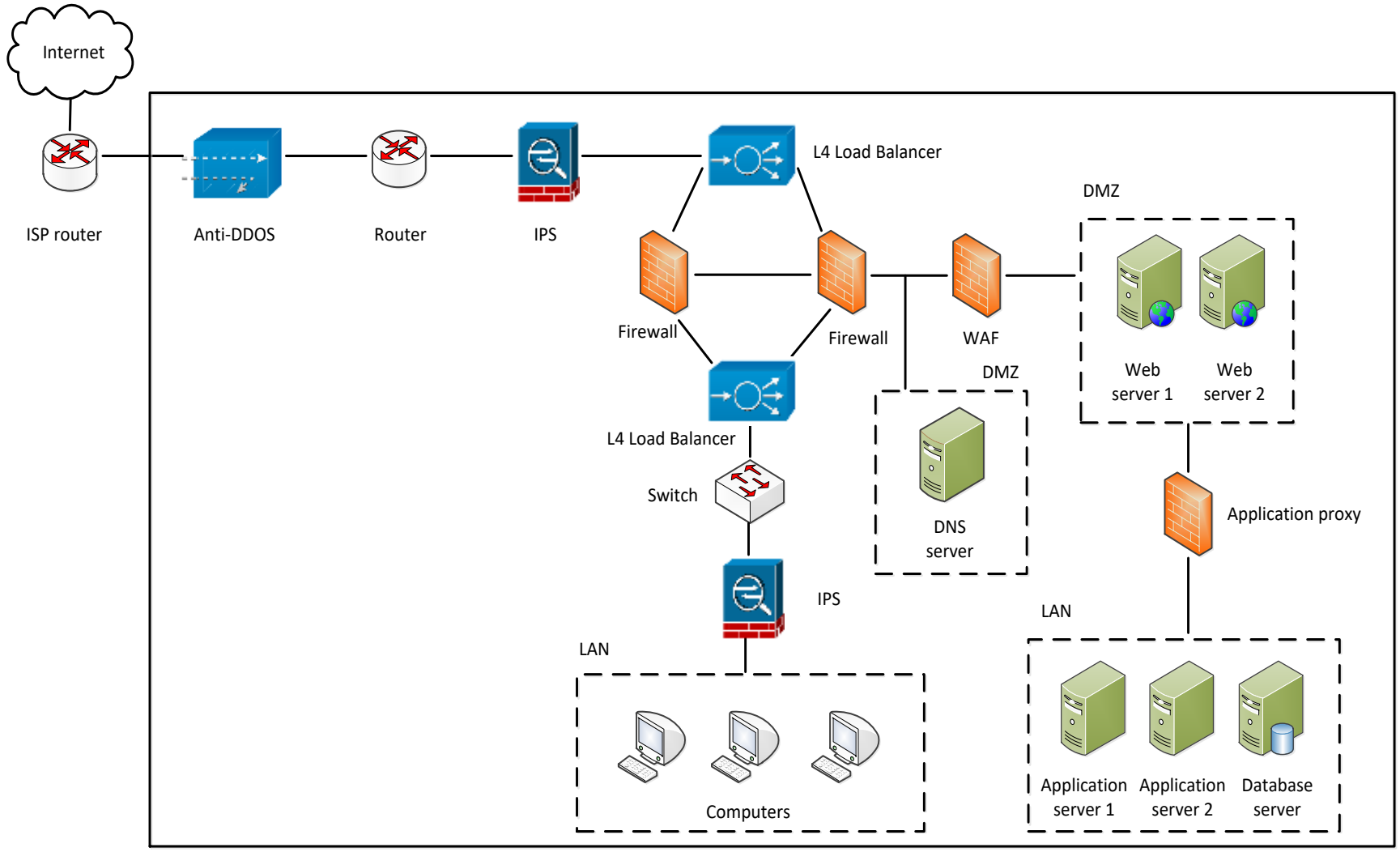


- DDoS: Distributed Denial of Service attacks
- WAF: Web Application Firewall
- DMZ: Demilitarized Zone

Q: Fundamental Security principles?

Q: Security mechanisms?

An example of security mechanisms (cont.)



- IPS: intrusion prevention system

Summary

- Security concepts
- Terminologies
- Functional requirements
- Security design principles (briefly)
- Security strategy
- Security mechanisms