CYBR3000

Applied Class 1: Cybersecurity Overview

Part I: Review Questions

1.1. CIA triad + AA.

Based on the description of each key objective below, select the most appropriate security goal from the following options: Confidentiality, Integrity, Availability, Authenticity, and Accountability.

Which security goal best matches each of the following scenarios?

(a) Protecting transmitted data from passive attacks such as message content disclosure and traffic analysis.

Answer:

(b) Ensuring that received data is exactly as sent by an authorized entity, with no modification, insertion, deletion, or replay.
Answer:

(c) Ensuring that information is accessible and usable when needed to fulfill its intended purpose.

Answer:

(d) Verifying that an entity or data is genuine and can be trusted.

Answer:

(e) Ensuring that actions performed by an entity can be uniquely traced back to that entity.

Answer:

1.2. Security terms and relationships.

Figure 1 shows the security terms and their relationships. Fill out the empty boxes with suitable terms.

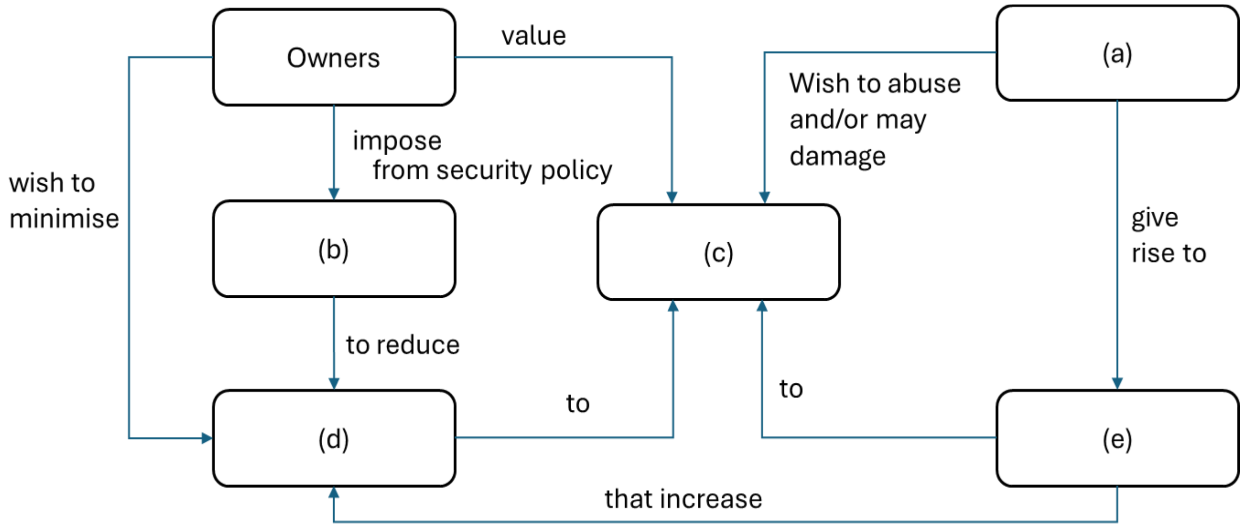

Figure 1. Security terms and relationships

(a)

(b)

(c)

(d)

(e)

1.3. Explain the following terms in brief.

(a) Give five high level examples of system resource (asset)

(b) Vulnerability

(c) Security policy

(d) Adversary

(e) Threat

(f) Attack

(g) Intrusion

(h) countermeasure / control

(i) risk

1.4. Answer the following questions.

a) What is the difference between active and pass attack?

b) What is the difference between inside and outside attack?

c) What is an attack surface? Give four examples of attack surfaces.

d) What is attack vector?

1.5. Fundamental Security Design Principles

This is a list of fundamental security principles:
(1) Complete mediation; (2) Economy of mechanism; (3) Encapsulation; (4) Fail-safe defaults; (5) Isolation; (6) Layering; (7) Least astonishment; (8) Least common mechanism; (9) Least privilege; (10) Modularity; (11) Open design; (12) Psychological acceptability; (13) Separation of privilege.

Which principle does this best illustrate? Choose only one correct number.

a) A system ensures that access checks are performed every time a subject attempts to access an object, rather than caching the result of a previous check.
b) A simple and small kernel is used to reduce the chance of errors and make the system easier to verify and maintain.
c) A system hides internal details and only exposes necessary interfaces to limit what external modules can access or modify.
d) By default, users are denied access to resources unless they are explicitly granted permission.
e) A virtual machine runs untrusted code in an environment that prevents it from interfering with the host system.
f) A system is designed with multiple levels of defense, where failure at one level can be caught by another.
g) A user interface avoids unexpected behavior and ensures that functions behave in ways users would naturally expect.
h) A system avoids sharing components like a single logging mechanism between high- and low-privilege processes to prevent leakage.
i) A user is only granted the minimal set of permissions necessary to perform their job.
j) A large application is broken into separate components so that each part can be developed, tested, and secured independently.
k) The design and security mechanisms of the system are open to the public and do not rely on secrecy for protection.
l) Security warnings are clear and easy to understand so that non-technical users can make safe decisions.
m) Access to a sensitive function requires two separate approvals from different users.

Part II: Advanced Problems

2.1. Develop an attack tree for gaining access to the contents of a smart phone. The tree must (1) have one goal, (2) contain both AND & OR nodes and (3) have at least 5 leaf nodes.

2.2. (optional) Find some research papers and find attack surfaces of an autonomous vehicle and list them. You may read the following papers:

- Nguyen et al. "AuSSE: A Novel Framework for Security and Safety Evaluation for Autonomous Vehicles." 2024 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S). IEEE, 2024.
- Kim et al. "Cybersecurity for autonomous vehicles: Review of attacks and defense." *Computers & security* 103 (2021): 102150.
- Clifford et al. "Autonomous Vehicle Security: Composing Attack, Defense, and Policy Surfaces." Proceedings of the 2022 New Security Paradigms Workshop. 2022.