System Security

Overview

System Security

Securing the **internal behavior of a computing system** — including operating systems, memory, processes, user privileges, file systems, and program execution.

The Bug That Divided Intel ……..

$$\frac{4,195,835}{3,145,727} = 1.3338204491362410002$$

The world of mathematics.

$$\frac{4,195,835}{3,145,727} = 1.3337390680902037589$$

The world from the Pentium's point of view.

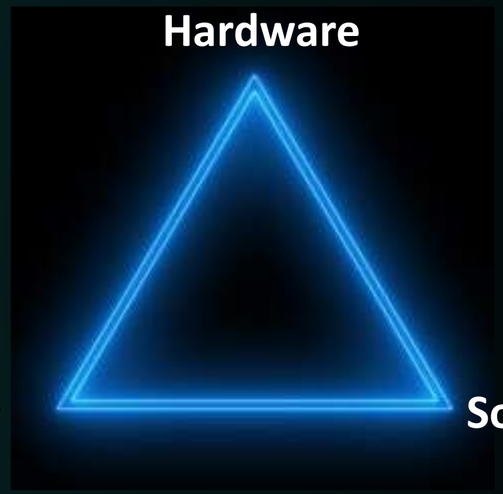
Feature	Details
Name	Intel Pentium FDIV Bug
Year	1994
Cause	Missing lookup table entries in FPU
Effect	Incorrect floating-point division results
Impact	$475 million recall; damaged Intel’s reputation
Lesson	Importance of thorough hardware testing

A single flaw in the heart of a processor can shake the confidence of the entire computing world

More …

- Heartbleed Bug (2014)
- The Therac-25 Radiation Machine (1985–1987)
- Ariane 5 Rocket Explosion (1996)
- Knight Capital Group Trading Bug (2012)

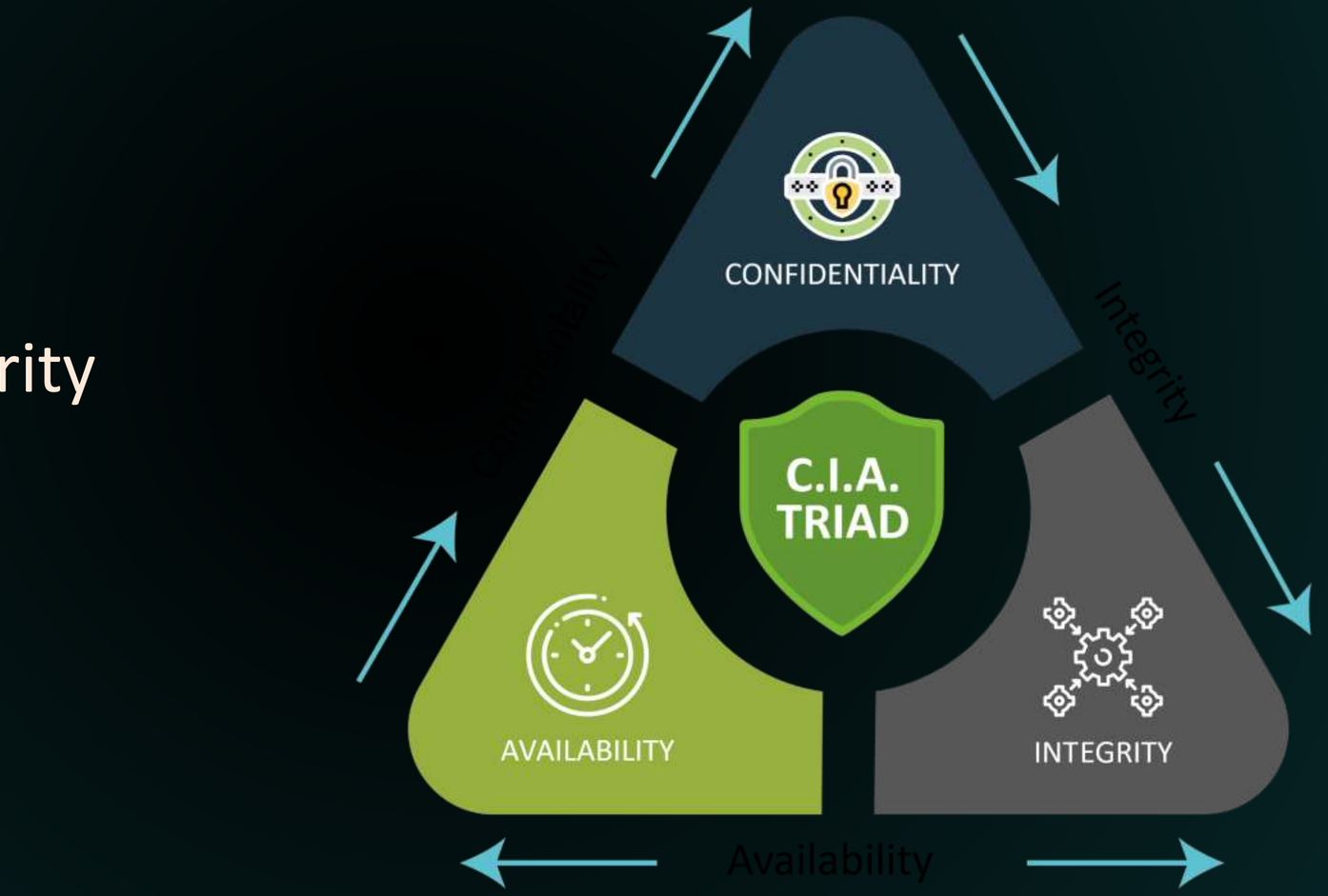
What to Attack – Components Affected



A threat is blocked by control of vulnerability

Security Goals

- The Authentication
- Authorization
- Confidentiality
- Data/message integrity
- Accountability
- Availability
- Non-repudiation



Scenarios for Analyzing Security Goals

Star Health reported receiving a $68,000 ransom demand following a data breach that resulted in the leak of customer data and medical records. Hackers released sensitive information via Telegram chatbots and a website, leading to an 11% decline in the company's shares.

Which security goals were violated?

Scenarios for Analyzing Security Goals

1. A government system uses mandatory access control (MAC) to classify documents.

A user with "Secret" clearance tries to read a "Top Secret" file but is denied.

Which security goal is most clearly enforced in this scenario?

A) Availability

B) Confidentiality

C) Integrity

D) Accountability

Scenarios for Analyzing Security Goals

1. A government system uses mandatory access control (MAC) to classify documents.

A user with "Secret" clearance tries to read a "Top Secret" file but is denied.

Which security goal is most clearly enforced in this scenario?

A) Availability

B) Confidentiality

C) Integrity

D) Accountability

Scenarios for Analyzing Security Goals

2. In a cloud system, data is encrypted at rest and during transmission, but the encryption keys are stored in plaintext on the same server.

Which security goal is technically implemented but practically violated?

A) Confidentiality

B) Integrity

C) Non-repudiation

D) Availability

Scenarios for Analyzing Security Goals

2. In a cloud system, data is encrypted at rest and during transmission, but the encryption keys are stored in plaintext on the same server.

Which security goal is technically implemented but practically violated?

A) Confidentiality

B) Integrity

C) Non-repudiation

D) Availability

Scenarios for Analyzing Security Goals

3. A developer modifies application logs to remove evidence of unauthorized data access.

Which TWO security goals are directly violated?

A) Confidentiality and Integrity

B) Integrity and Accountability

C) Availability and Non-repudiation

D) Non-repudiation and Anonymity

Scenarios for Analyzing Security Goals

3. A developer modifies application logs to remove evidence of unauthorized data access.

Which TWO security goals are directly violated?

A) Confidentiality and Integrity

B) Integrity and Accountability

C) Availability and Non-repudiation

D) Non-repudiation and Anonymity

Scenarios for Analyzing Security Goals

4. A ransomware attack encrypts all patient records in a hospital and demands payment. Backups were also deleted.

Which of the following statements is most accurate?

A) Only availability is affected

B) Both confidentiality and accountability are impacted

C) Integrity, availability, and possibly confidentiality are all compromised

D) This is an authorization failure only

Scenarios for Analyzing Security Goals

4. A ransomware attack encrypts all patient records in a hospital and demands payment. Backups were also deleted.

Which of the following statements is most accurate?

A) Only availability is affected

B) Both confidentiality and accountability are impacted

C) Integrity, availability, and possibly confidentiality are all compromised

D) This is an authorization failure only