SENG 11232 · Engineering Foundation

STUDENT PRE-LECTURE NOTES · LECTURE 11

Engineering Safety, Security & Ethics

Module 4 — Networks, Security & Professional Practice

HOW TO USE Read these notes BEFORE the lecture. Highlight terms you don't recognise. Bring your questions to class. Use the blank spaces for your own notes.

Learning Objectives

By the end of this lecture, you should be able to:

- 1. Explain safety-critical software and describe consequences of failure
- 2. Apply the CIA triad to assess security requirements
- 3. Identify and describe the OWASP Top 10 vulnerabilities
- 4. Apply secure design principles: least privilege, fail-safe defaults
- 5. Describe GDPR obligations and open source licensing

Safety-Critical Software

Famous Failures

- Therac-25 (1985-87): race condition in radiation therapy machine; 6 patients killed
- Ariane 5 (1996): 64-bit float → 16-bit int overflow; $370M rocket destroyed
- Boeing 737 MAX MCAS (2018-19): single-sensor reliance; 346 killed
- UK Post Office Horizon (1999-2019): software bugs; 736 wrongful convictions

Safety Engineering Principles

- Fail-safe: on any failure, move to a safe state
- Fault tolerance: continue operating despite component failures
- Defence in depth: multiple independent safety layers

KEY Safety must be designed in from the start. You cannot test safety into a system after it is built.

Your notes:

____

____

____

Security Engineering

CIA Triad

- Confidentiality: only authorised parties access data (encryption, access control)
- Integrity: data is accurate and unmodified (hashes, digital signatures)
- Availability: systems accessible when needed (redundancy, DDoS protection)

OWASP Top 10 (selected)

- A01 Broken Access Control: most common — users access resources they should not
- A03 Injection: SQL/command injection — user input treated as code
- A04 Insecure Design: security not considered in architecture

Secure Design Principles

- Least privilege: grant minimum permissions necessary
- Fail securely: on error, deny access by default
- Never trust user input: validate, sanitise, parameterise all inputs

NOTE GDPR: personal data must be protected; privacy by design and by default is a legal requirement in the EU. Fines up to 4% of global annual revenue.

Your notes:

____

____

____

Key Terms for This Lecture

Term	Your Definition (fill in during/after lecture)
Safety-Critical Software	
Fail-Safe	
Fault Tolerance	
CIA Triad	
Confidentiality	
Integrity	
Availability	
OWASP	
SQL Injection	
Least Privilege	
GDPR	
Privacy by Design	
Open Source Licence	

Self-Check Questions

Answer these after the lecture to test your understanding:

- Q1. Identify the root cause of the Therac-25 failures and state which engineering principle was violated.

Answer: ____

- Q2. Explain the CIA triad with one real-world threat to each property.

Answer: ______________________________

- Q3. What is SQL injection? Write an example vulnerable query and the parameterised fix.

Answer: ______________________________

- Q4. Under GDPR, what does "privacy by design" require of a software engineer building a user registration system?

Answer: ______________________________

SENG 11232 Engineering Foundation · Lecture 11: Engineering Safety, Security & Ethics