PRESENTATION

Group 11

INTRODUCTION

- A Trusted System is a system that correctly enforces a defined security policy.
- It ensures:
    - Confidentiality
    - Integrity
    - Availability
-
- Used in modern communication systems like cloud messaging, email platforms, and enterprise collaboration tools.
- Core components:
    - Trusted Computing Base (TCB) – hardware + software enforcing security
    - Security Kernel – core mechanism implementing access control
    - Reference Monitor – checks every access request
-

DATA ACCESS CONTROL

- Regulates who can access what data and what operations they can perform.
- Operations include: Read, Write, Execute, Modify.

Access Control Models:

- Discretionary Access Control (DAC) - Owner decides access
- Mandatory Access Control (MAC) - Based on security labels
- Role-Based Access Control (RBAC) - Based on user roles
- Attribute-Based Access Control (ABAC) - Based on user, resource, and environmental attributes
- Prevents:
  - Unauthorized access
  - Data leakage
  - Insider misuse

TROJAN HORSE & DEFENSE MECHANISMS

Trojan Horse:

- Malicious software disguised as legitimate program
- Can:
    - Steal data
    - Capture passwords
    - Create backdoors
    - Misuse user privilege
    -

Defense Mechanisms:

- Principle of Least Privilege
- Mandatory Access Control
- Sandboxing
- Code Signing
- Continuous Monitoring & Auditing

CASE STUDY

Case Study: Cloud Communication Platform

- User logs in with Multi-Factor Authentication
- Identity verified using IAM
- Access controlled using RBAC/ABAC
- Data encrypted in transit (TLS)
- Applications sandboxed
- Suspicious activity → session terminated

Result:

- Secure communication
- Controlled data access
- Reduced malware impact