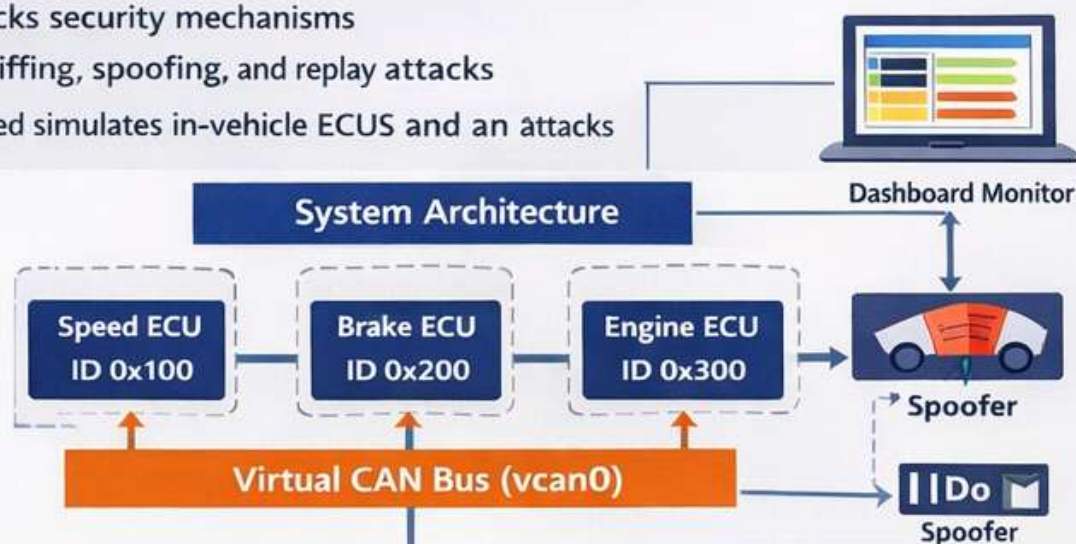


Simulating CAN Bus Attacks and Defences in a Virtual Environment

Ana Chicaiza | Advanced Cybersecurity | Supervisor: Md Sadeque

CAN Bus Vulnerabilities & Simulation Overview

- CAN bus lacks security mechanisms
- Prone to sniffing, spoofing, and replay attacks
- Virtual testbed simulates in-vehicle ECUS and an attacks



Cyber Attacks Demonstrated

Sniffing

- Eavesdropping on CAN traffic



Spoofing

- Injecting fake speed data (ID 0x100)

Spoofed Speed
120 kmh

Replay

- Resending previously captured frames



Defensive Mechanisms Implemented

ID Whitelisting

- Allow only approved IDs



Flood Detection

- Detect rapid message bursts



Anomaly Logging

FLOOD ALERT:
High Traffic Rate



ALERT:
Anomalous Behaviour

Results & Conclusions

- Spoofed and replayed messages manipulated ECU behaviour
- Defensive measures detected but did not block all attacks
- **Future Work:**
 - Enhance intrusion detection
 - Integrate cryptographic security