

Project

Applying Your Learning

Lab9

Remember

There is no 100% security

Security, like all engineering, involves tradeoffs

Know what you are trying to secure

The adversary...



**State
Sponsored**

Project -- Randomizer

Network	Number of Nodes per Session	Nature of Security	Channel	Hardware Acceleration	Message Rate
CAN	Fixed; N=5	Secure each message	1	Symmetric only	10 msg/sec
CAN FD	Dynamic; N=3..15	Secure the control loop	8	Symm & Asymm	1,000 msg/sec

Project – Randomizer Results

Student 1

CAN
Dynamic; N = 3..15
Secure Each Message
1 Channel
Symm and Asymm
1000 msg/sec

Student 2

CAN
Fixed; N = 5
Secure Each Message
1 Channel
Symm Only
1000 msg/sec

Student 3

CAN
Dynamic; N = 3..15
Secure the Control Loop
8 Channels
Symm Only
1000 msg/sec

Student 4

CAN FD
Fixed; N = 5
Secure Each Message
8 Channels
Symm and Asymm
10 msg/sec

Student 5

CAN FD
Dynamic; N = 3..15
Secure the Control Loop
1 Channel
Symm Only
1000 msg/sec

Student 6

CAN
Dynamic; N = 3..15
Secure Each Message
1 Channel
Symm and Asymm
10 msg/sec

Schedule

- 12 APR Topic Review / Project Launch
- 19 APR [DEFEND] Design Review: **Key Management**
- 26 APR [DEFEND] Design Review: **Secure Message Exchange**
- 03MAY [ATTACK] Analysis: **Attack Plan for Two Designs**

Administration

- For each design review
 - Post an updated slide deck (~3 slides) to MS Teams
 - The review will have a Q&A component
- For attack plan
 - Are there weaknesses in the design concept?
 - Are there weaknesses in a likely embedded implementation?
 - Consider Meddler-in-the-Middle (MitM)
 - Consider the difficulty in Key Management