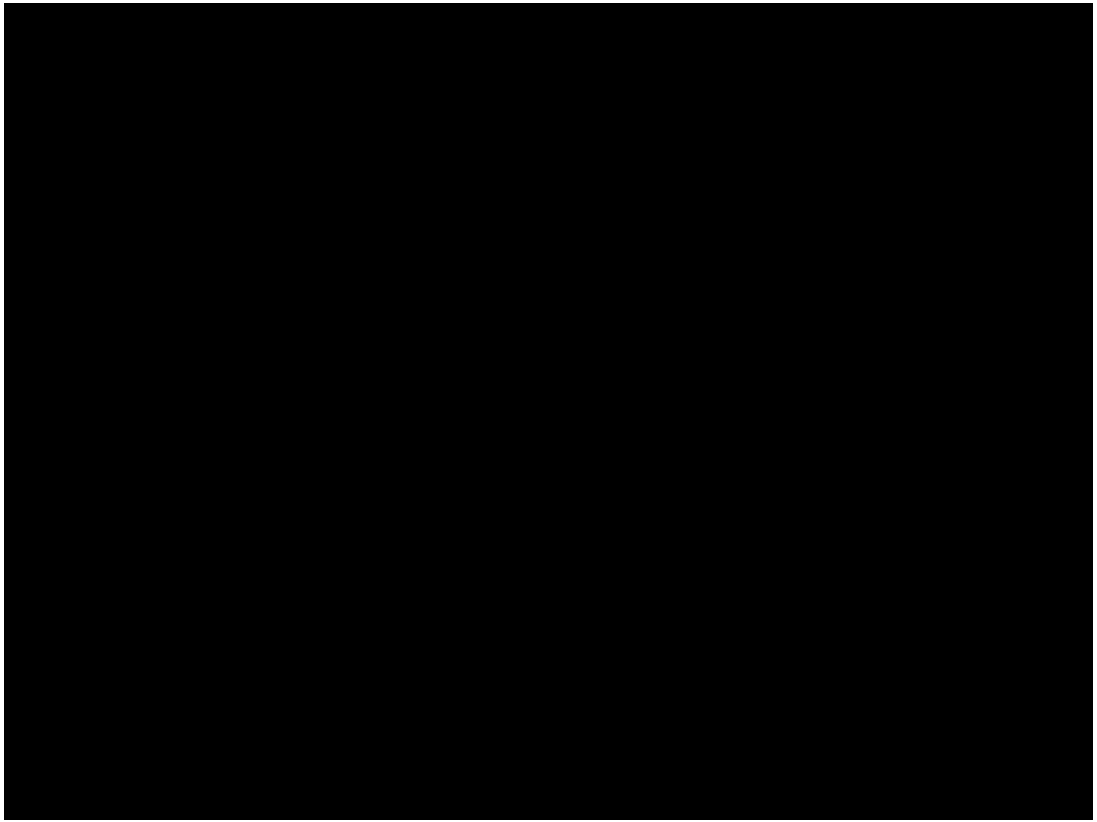
Blue Team Tricks - An overview of Automotive Defensive Engineering

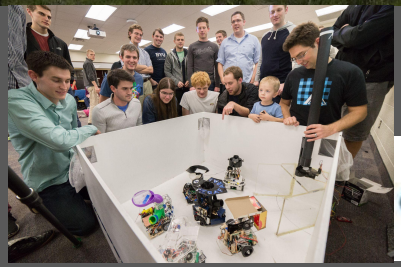
Who Am I?




STRANGER
THINGS

Raytheon

nuro



Ford CYBER SECURITY

RUSTIC SECURITY LLC
DESIGN, IMPLEMENT, VERIFY

NORTHROP GRUMMAN
Orbital ATK

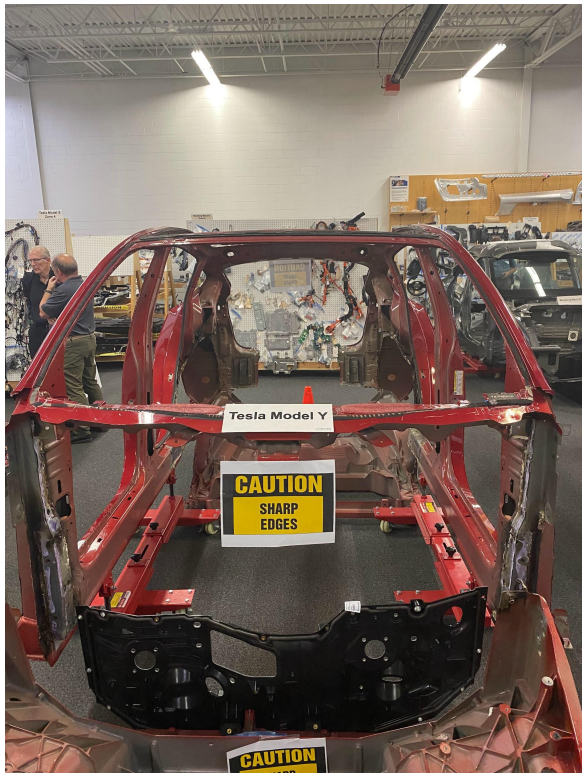
APTIV

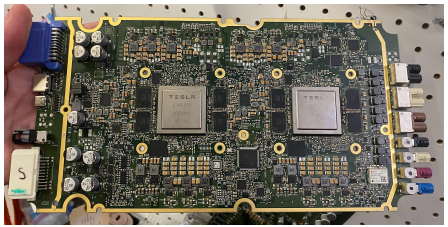
Sun Tzu said:

"If you know the enemy and know yourself, **you need not fear the result of a hundred battles**. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

https://www.facebook.com/suntzupage/

Defensive Security Overview





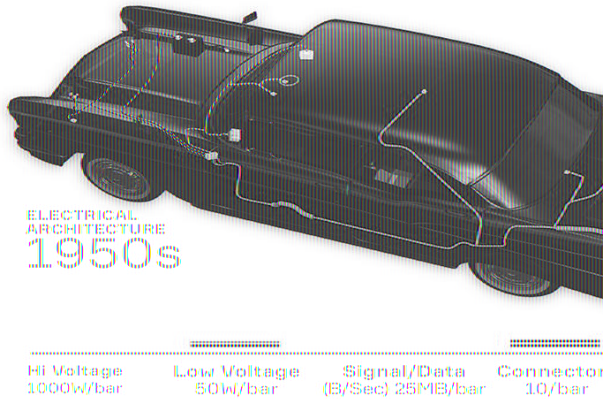
ECUs

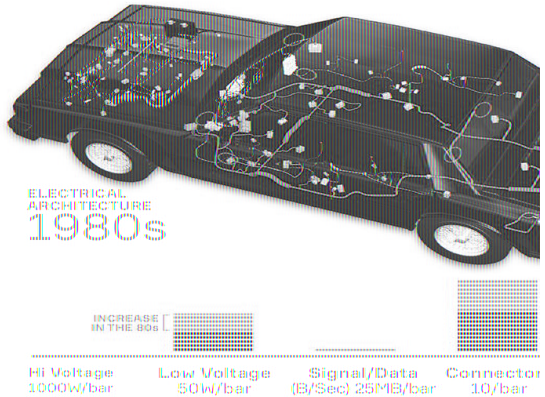
Vehicle
Networks

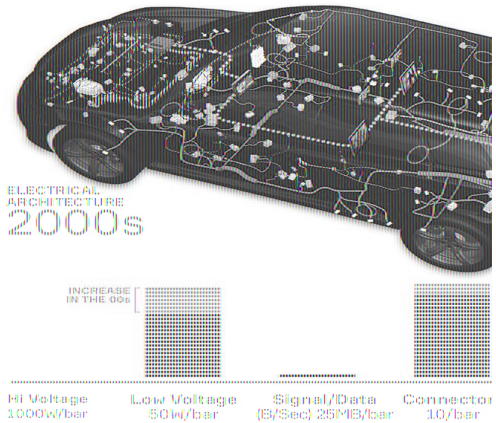
MUNRO

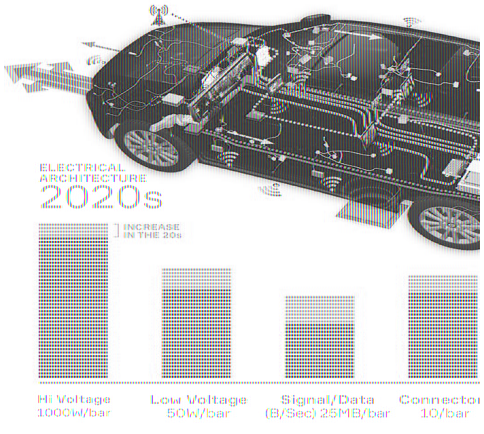
Evolution of Vehicle Architecture

https://www.aptiv.com/en/insights/article/evolution-of-vehicle-architecture

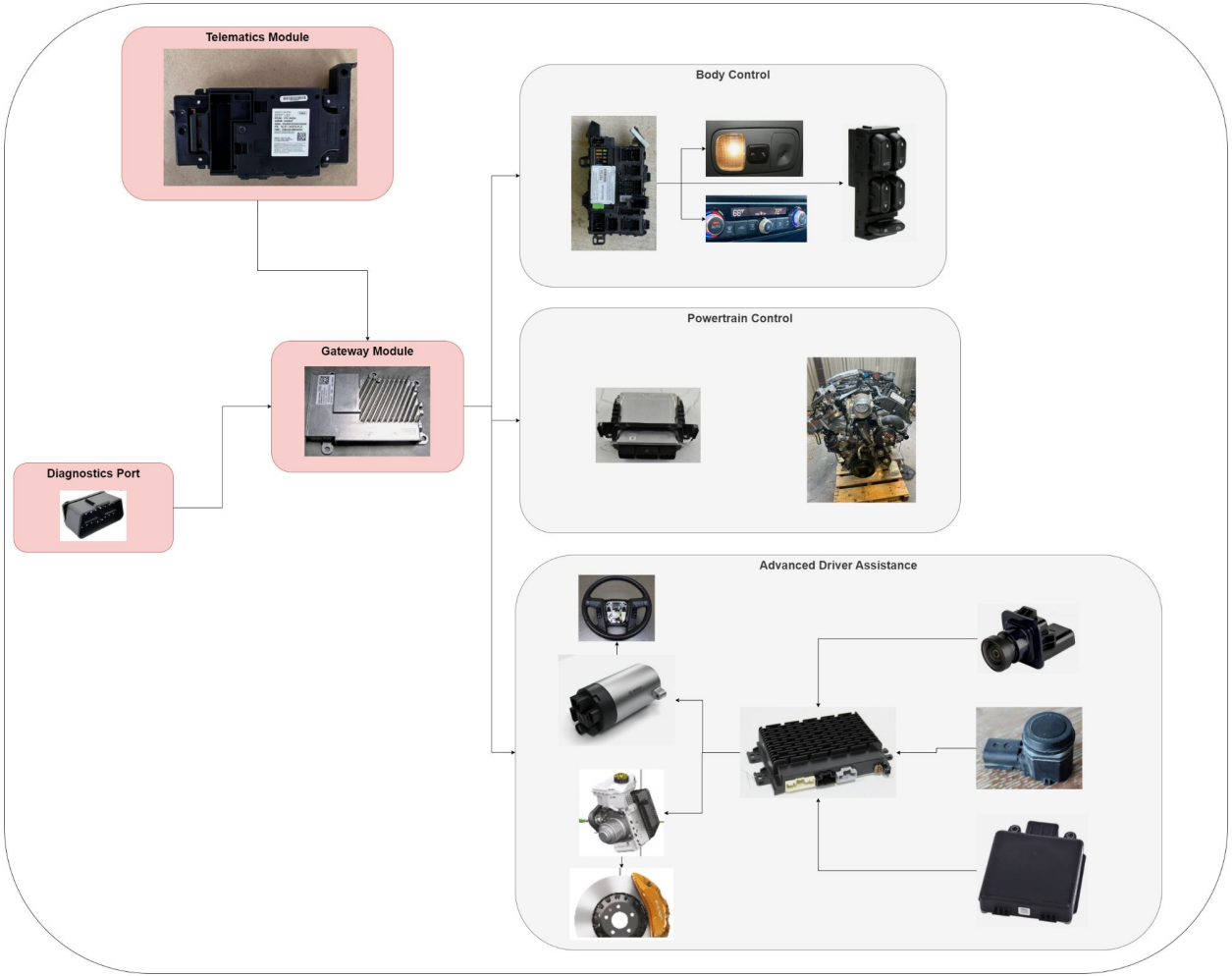








APTIV



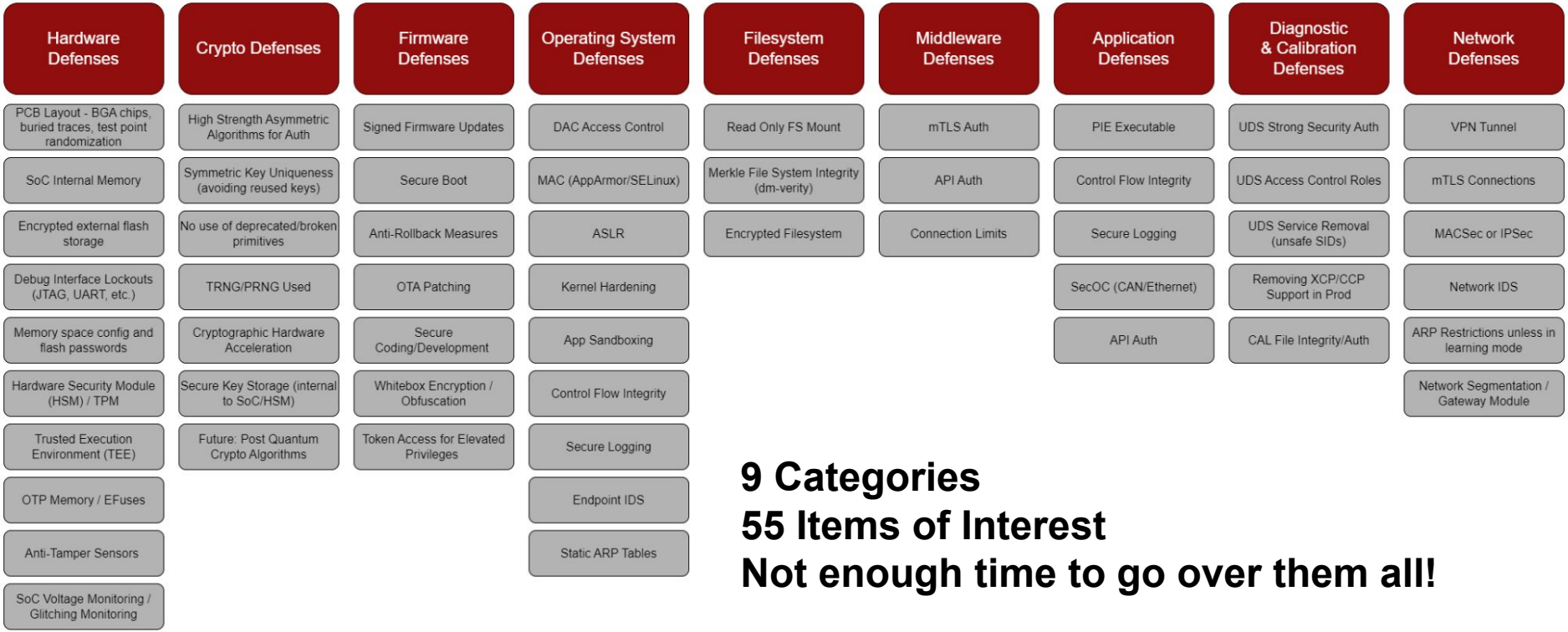
Functional Domains and Vehicle Architecture

Q - How do we secure a modern connected vehicle?

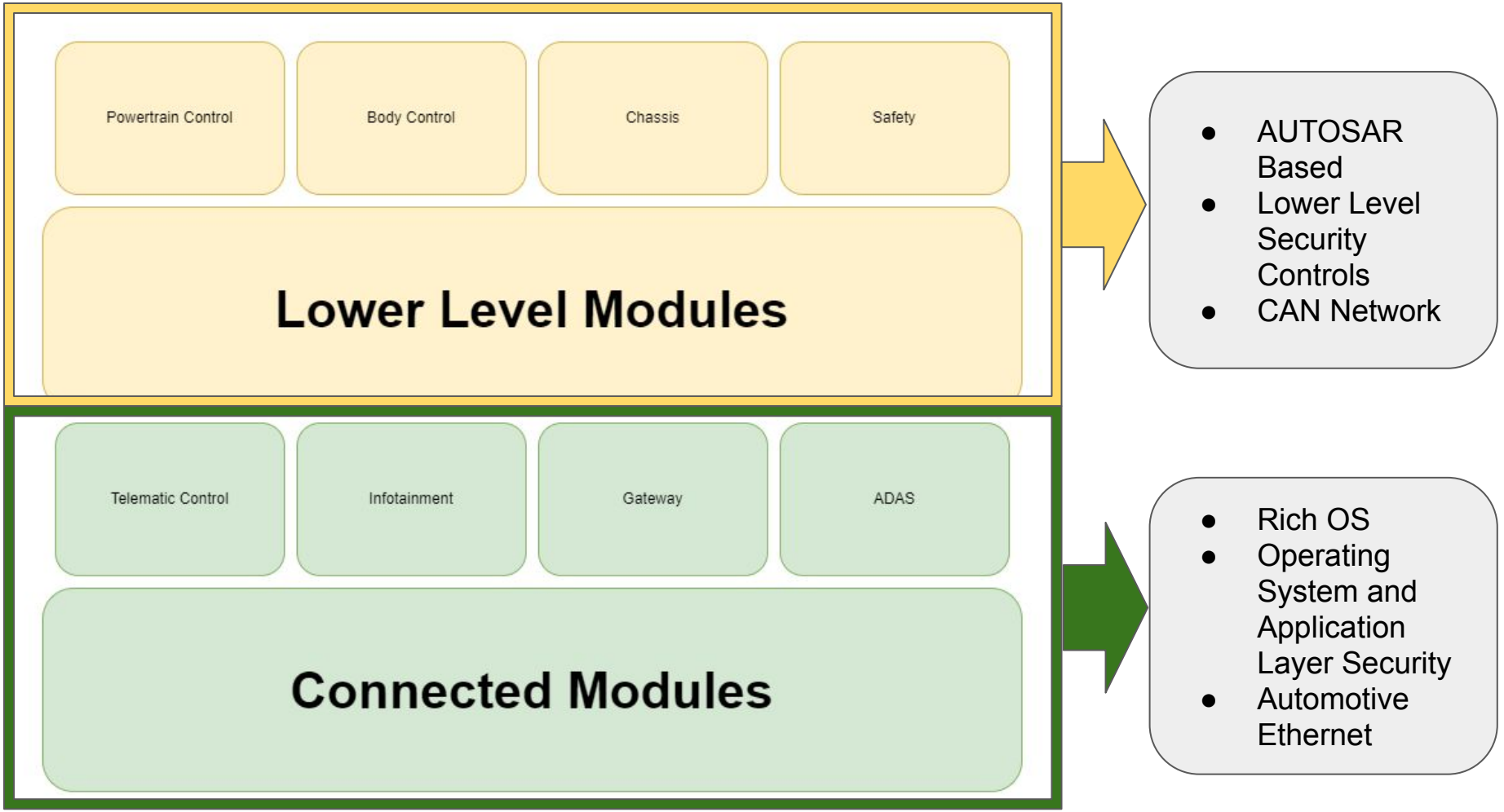

Ford

What's the risk and how much money do I have?


FORD

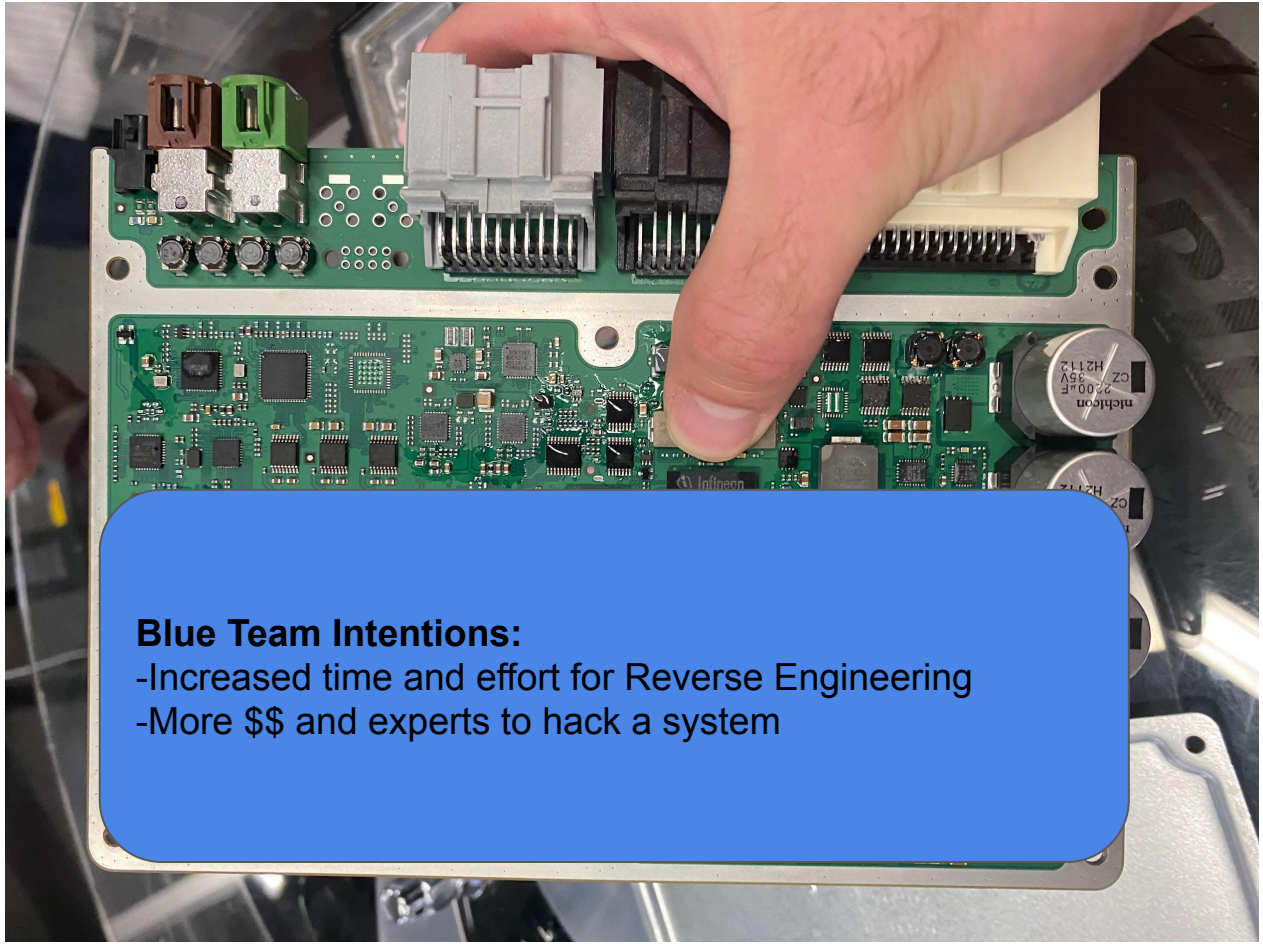


9 Categories
55 Items of Interest
Not enough time to go over them all!


Powertrain Control
Body Control
Chassis
Safety
Lower Level Modules
Telematic Control
Infotainment
Gateway
ADAS
Connected Modules
AUTOSAR Based
Lower Level Security Controls
CAN Network
Rich OS
Operating System and Application Layer Security
Automotive Ethernet

Hardware Defenses

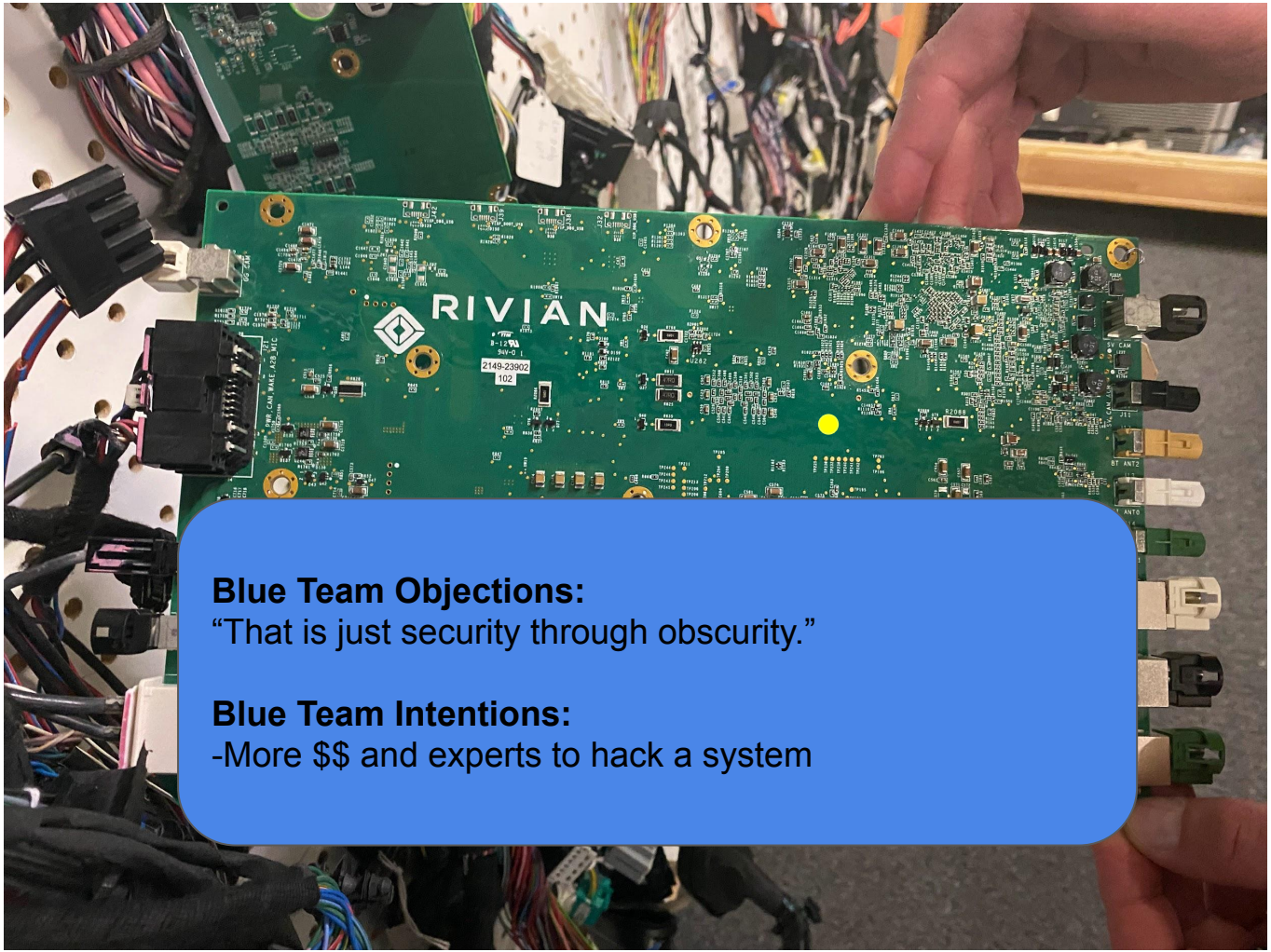
- PCB Layout - BGA chips, buried traces, test point randomization
- SoC Internal Memory
- Encrypted external flash storage
- Debug Interface Lockouts (JTAG, UART, etc.)
- Memory space config and flash passwords
- Hardware Security Module (HSM) / TPM
- Trusted Execution Environment (TEE)
- OTP Memory / EFuses
- Anti-Tamper Sensors
- SoC Voltage Monitoring / Glitching Monitoring



Blue Team Intentions:
-Increased time and effort for Reverse Engineering
-More $$ and experts to hack a system

Hardware Defenses

- PCB Layout - BGA chips, buried traces, test point randomization
- SoC Internal Memory
- Encrypted external flash storage
- Debug Interface Lockouts (JTAG, UART, etc.)
- Memory space config and flash passwords
- Hardware Security Module (HSM) / TPM
- Trusted Execution Environment (TEE)
- OTP Memory / EFuses
- Anti-Tamper Sensors
- SoC Voltage Monitoring / Glitching Monitoring

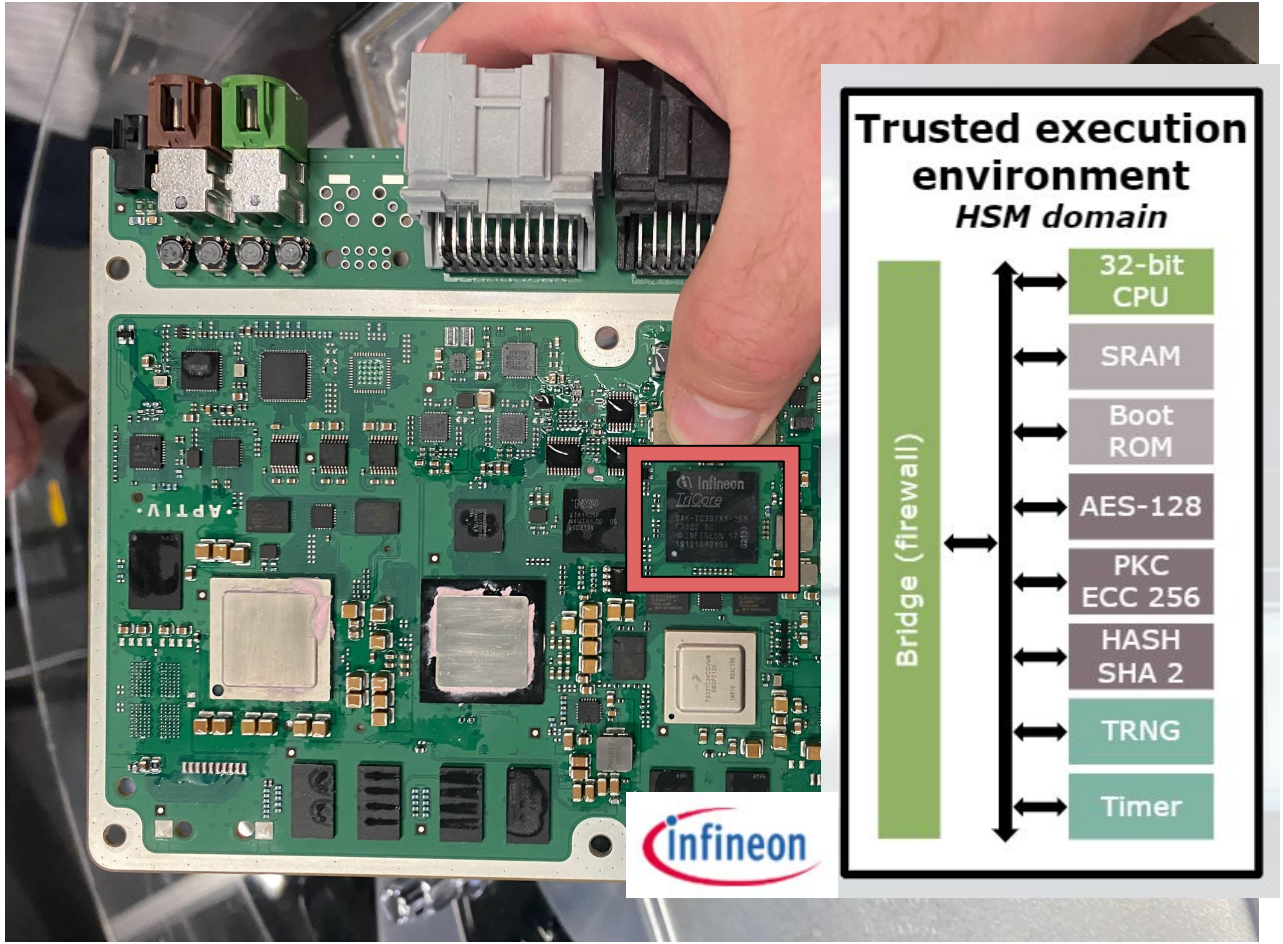


Blue Team Objections:
“That is just security through obscurity.”

Blue Team Intentions:
-More $$ and experts to hack a system

Hardware Defenses

- PCB Layout - BGA chips, buried traces, test point randomization
- SoC Internal Memory
- Encrypted external flash storage
- Debug Interface Lockouts (JTAG, UART, etc.)
- Memory space config and flash passwords
- **Hardware Security Module (HSM) / TPM**
- Trusted Execution Environment (TEE)
- OTP Memory / EFuses
- Anti-Tamper Sensors
- SoC Voltage Monitoring / Glitching Monitoring

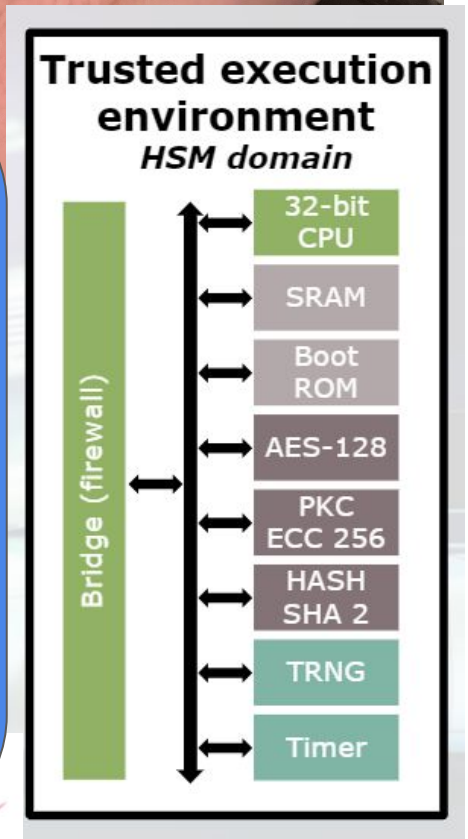


https://www.infineon.com/cms/media/eLearning/Automotive/aurix-hardware-security/presentation_html5.html?lms=1

Crypto Defenses

- High Strength Asymmetric Algorithms for Auth
- Symmetric Key Uniqueness (avoiding reused keys)
- No use of deprecated/broken primitives
- TRNG/PRNG Used
- Cryptographic Hardware Acceleration
- Secure Key Storage (internal to SoC/HSM)
- Future: Post Quantum Crypto Algorithms

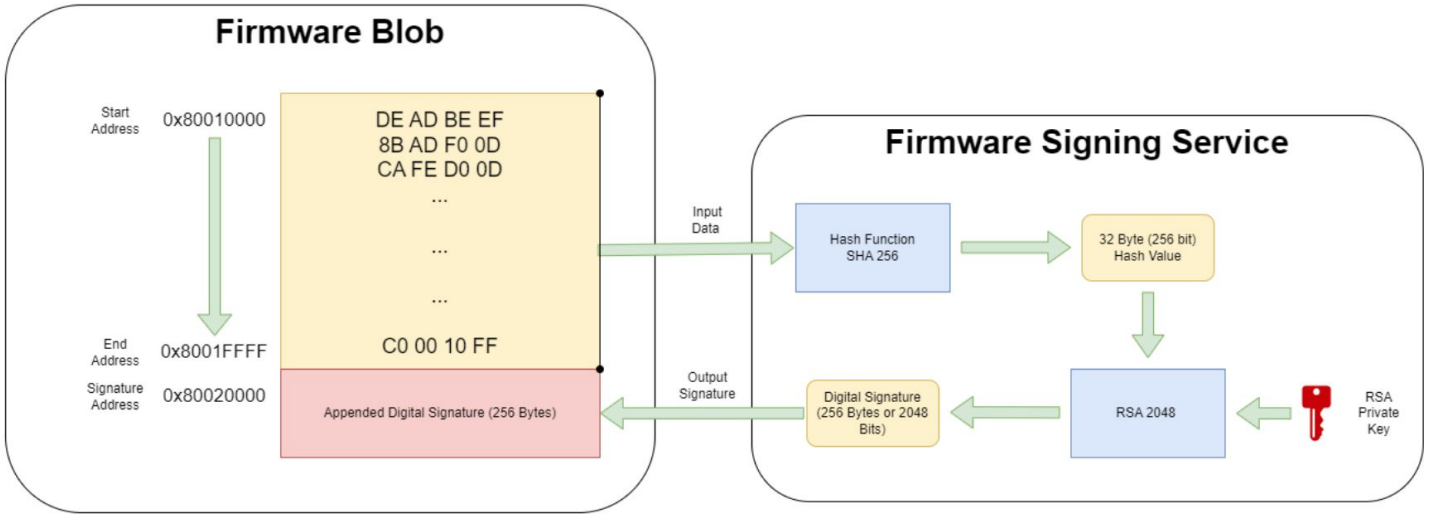
Blue Team Intentions:
-Architecturally separate host applications from security critical processing

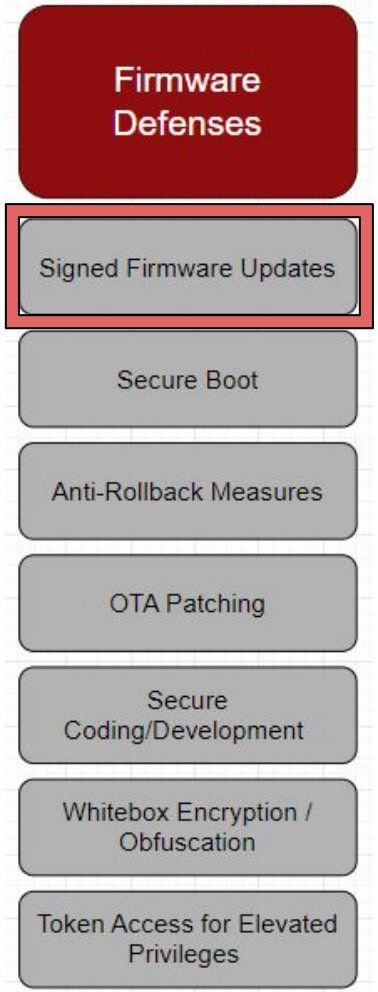


https://www.infineon.com/cms/media/eLearning/Automotive/aurix-hardware-security/presentation_html5.html?lms=1

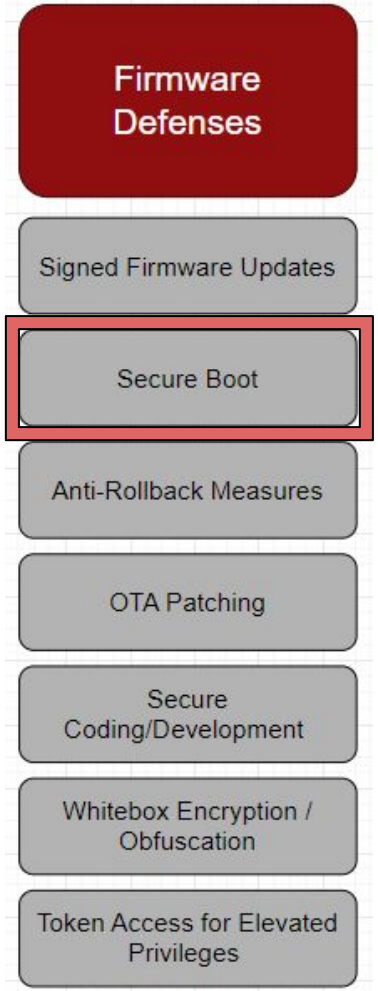
Firmware Defenses

- Signed Firmware Updates
- Secure Boot
- Anti-Rollback Measures
- OTA Patching
- Secure Coding/Development
- Whitebox Encryption / Obfuscation
- Token Access for Elevated Privileges

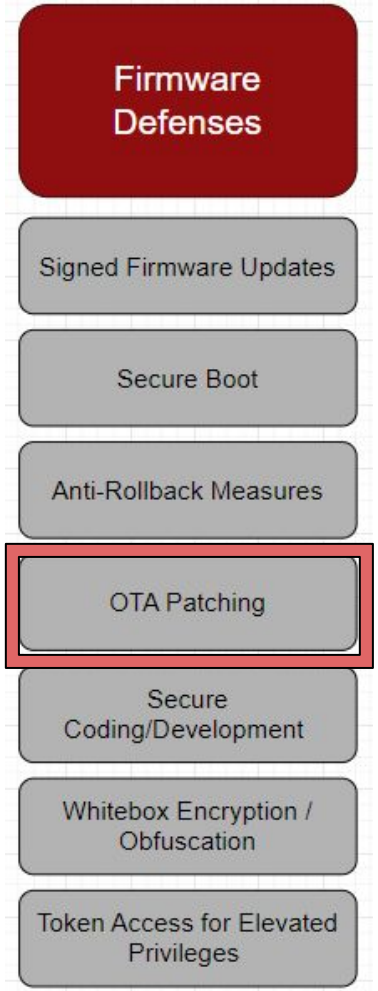




Blue Team Intentions:
-Stop backdoored firmware from being accepted by update process



Blue Team Intentions:
-Catch malicious firmware modifications at boot time
-Ensure firmware integrity

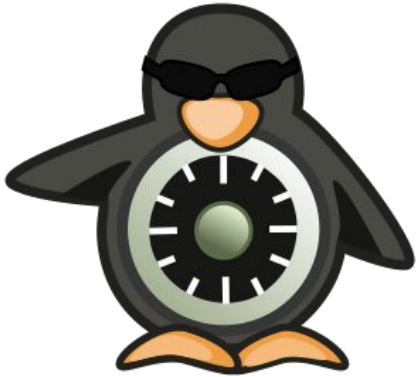


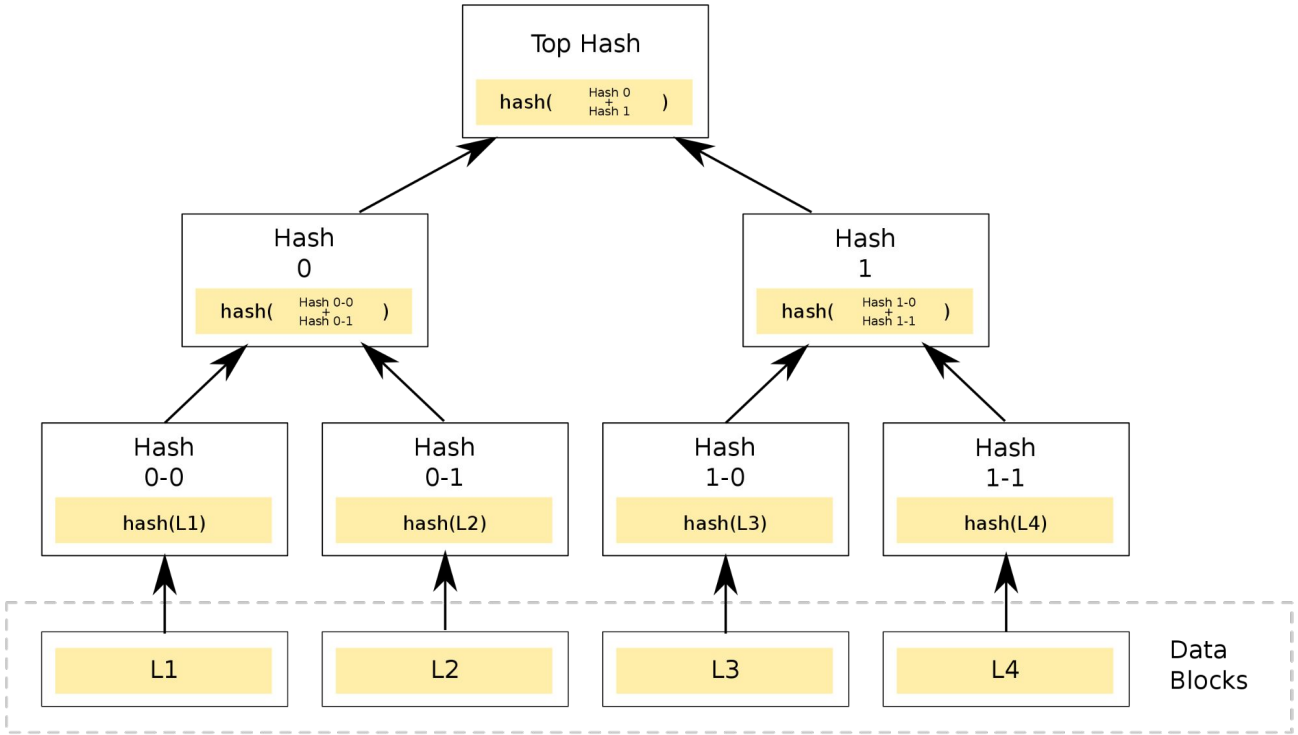
Blue Team Intentions:
-Frustrate attackers by patching firmware they may have spent a lot of time developing an exploit for

Operating System Defenses

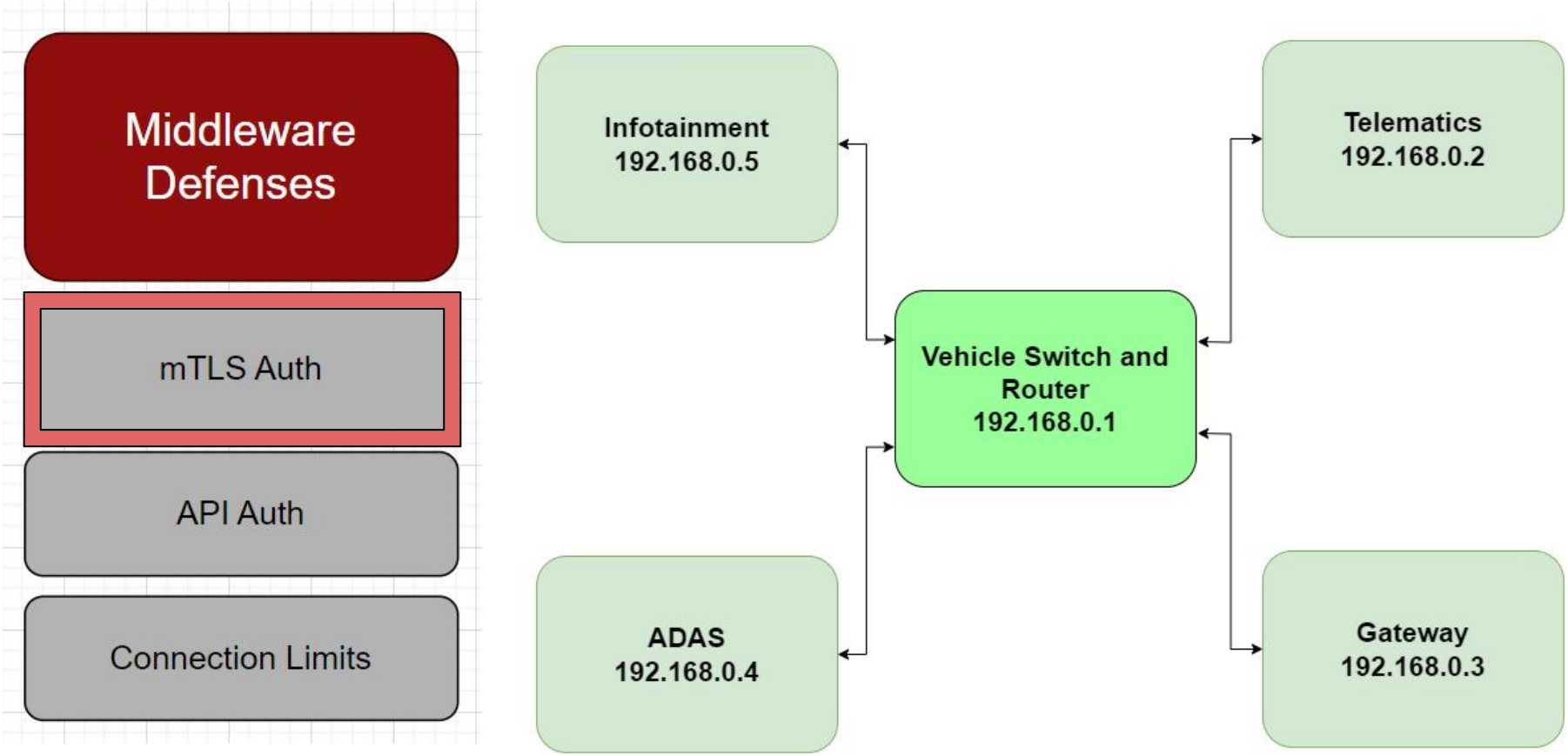
- DAC Access Control
- MAC (AppArmor/SELinux)
- ASLR
- Kernel Hardening
- App Sandboxing
- Control Flow Integrity
- Secure Logging
- Endpoint IDS
- Static ARP Tables

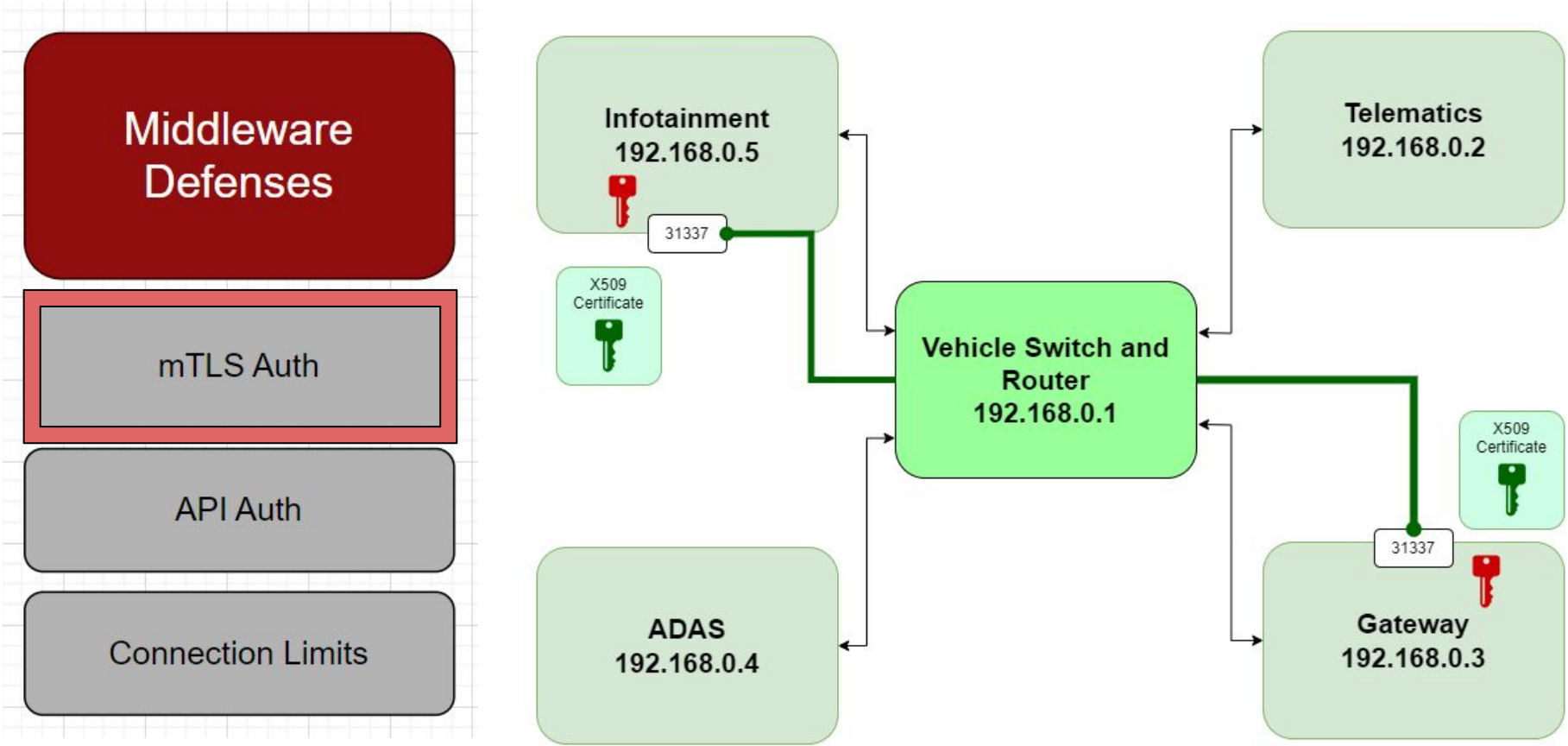
- Restricting access to the resources an application has access to
- If you find a vulnerability in an application, you still need to elevate privileges

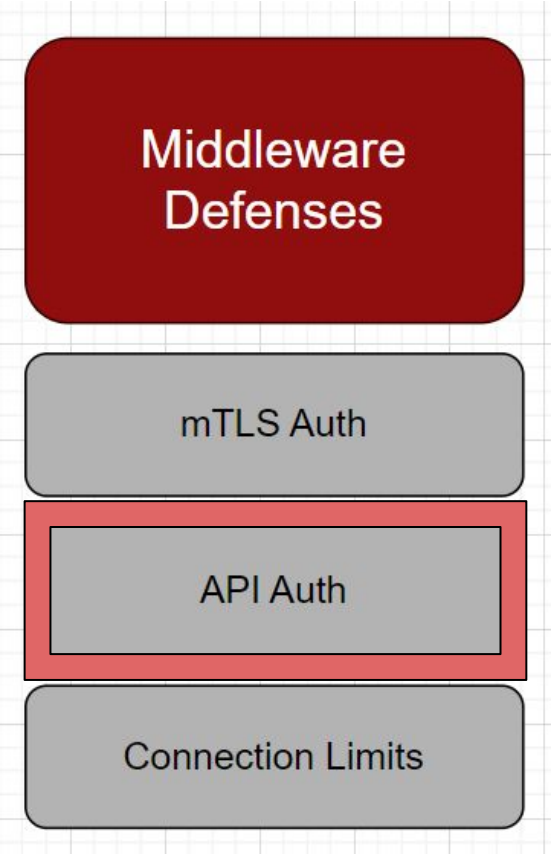


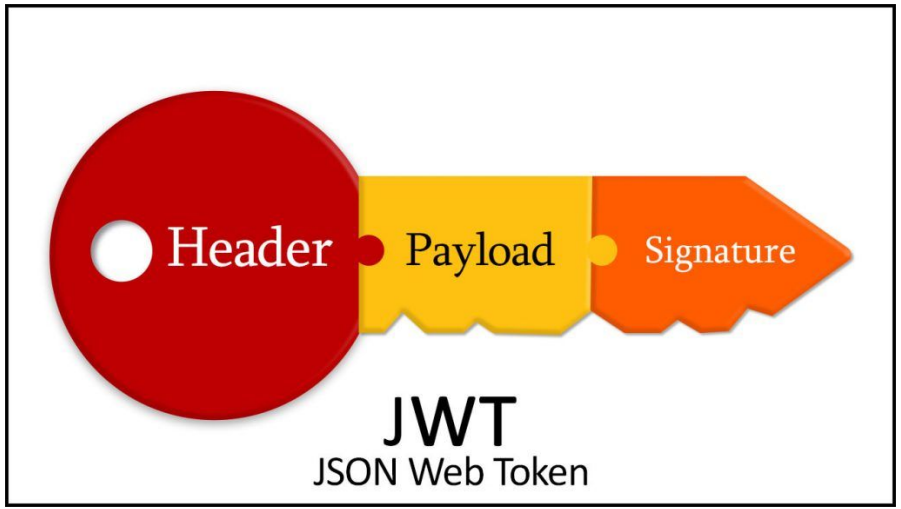


https://en.wikipedia.org/wiki/Merkle_tree#/media/File:Hash_Tree.svg

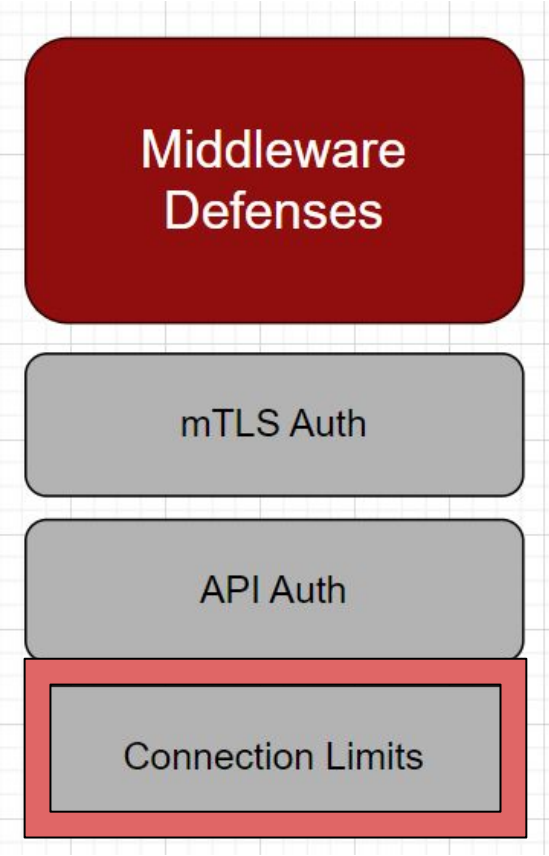

Middleware Defenses
mTLS Auth
API Auth
Connection Limits
Infotainment
192.168.0.5
Telematics
192.168.0.2
Vehicle Switch and Router
192.168.0.1
ADAS
192.168.0.4
Gateway
192.168.0.3


Middleware Defenses
mTLS Auth
API Auth
Connection Limits
Infotainment
192.168.0.5
31337
X509 Certificate
Telematics
192.168.0.2
Vehicle Switch and Router
192.168.0.1
ADAS
192.168.0.4
X509 Certificate
31337
Gateway
192.168.0.3

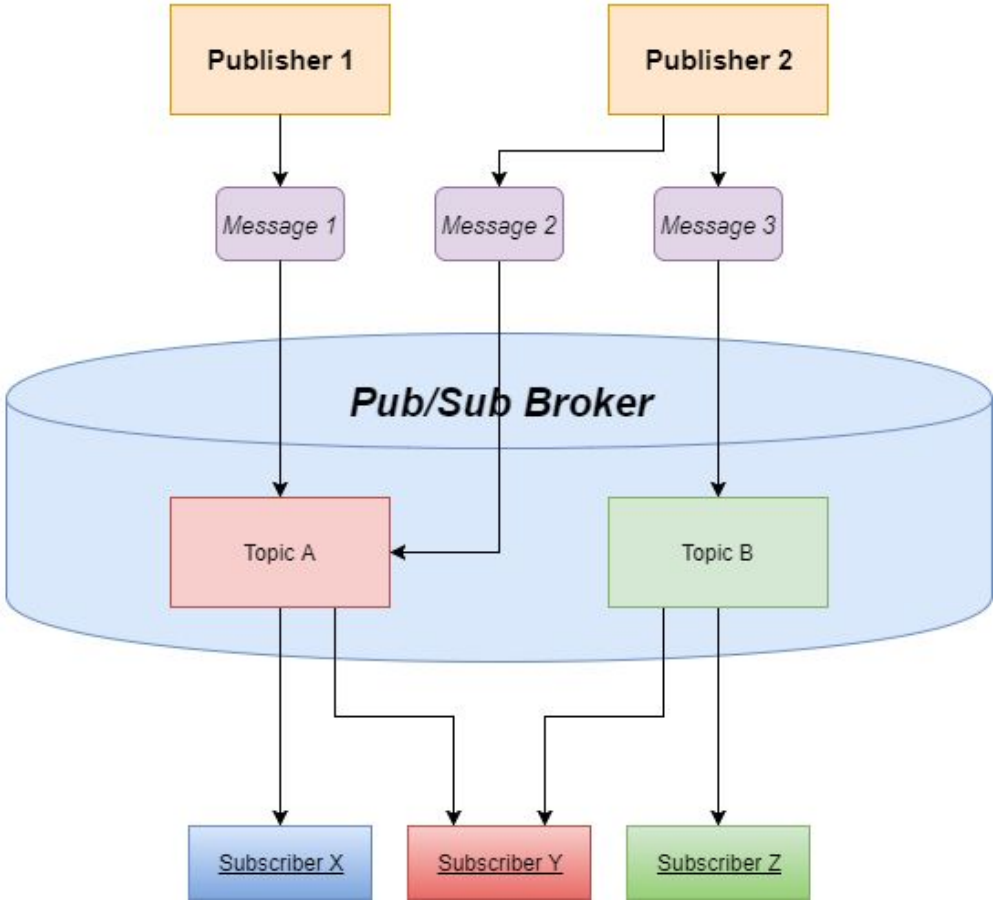




https://ansibytecode.com/jwt-peek-into-the-jargon-java-web-token/



Pub/Sub Broker



https://github.com/IAmMorrow/grpc-pubsub-broker

Application Defenses

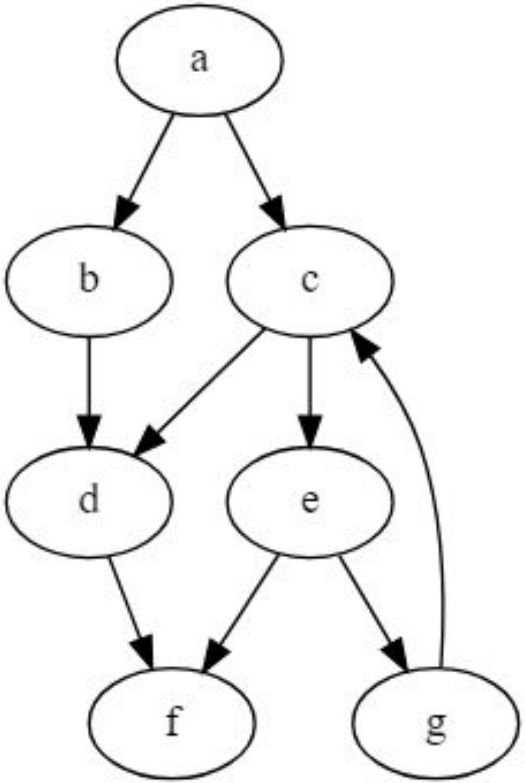
PIE Executable

Control Flow Integrity

Secure Logging

SecOC (CAN/Ethernet)

API Auth



- Shadow Stacks
- Lock Step Execution
- Stack Canaries
- Control flow graph execution monitoring

Application Defenses

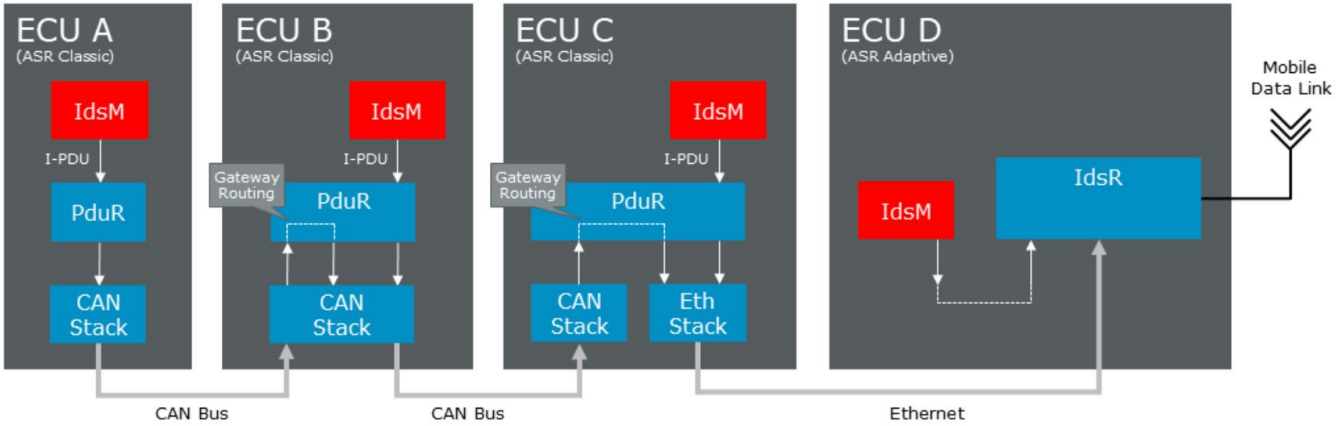
PIE Executable

Control Flow Integrity

Secure Logging

SecOC (CAN/Ethernet)

API Auth



https://www.autosar.org/fileadmin/standards/R20-11/FO/AUTOSAR_PRS_IntrusionDetectionSystem.pdf

Application Defenses

PIE Executable

Control Flow Integrity

Secure Logging

SecOC (CAN/Ethernet)

API Auth

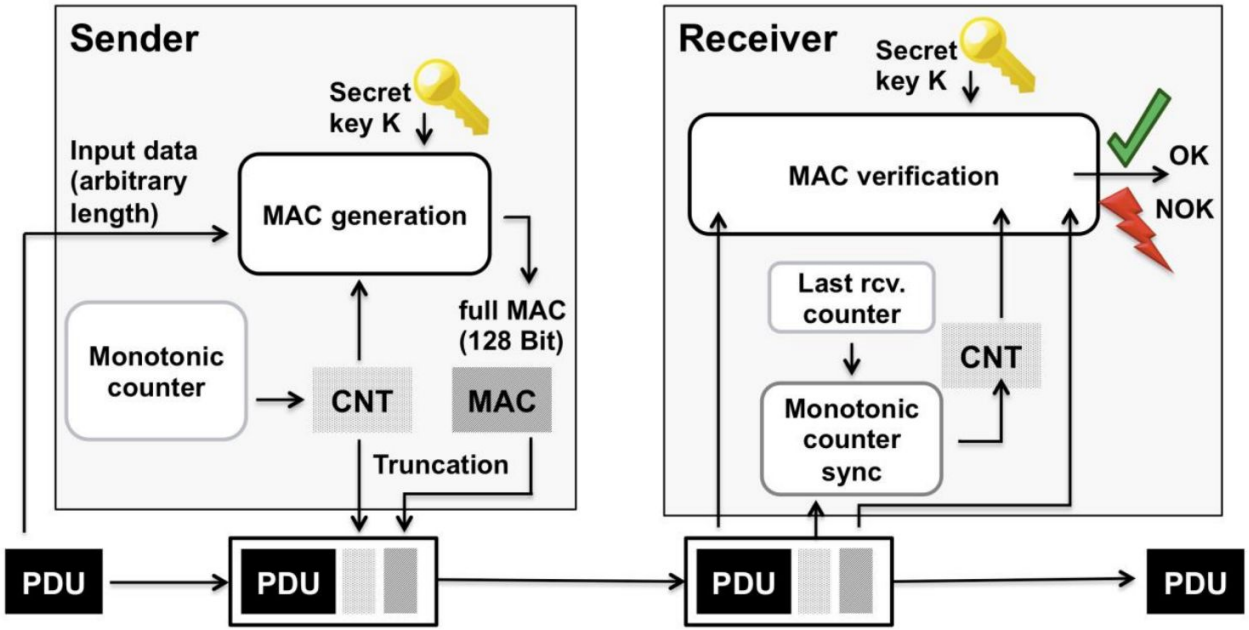
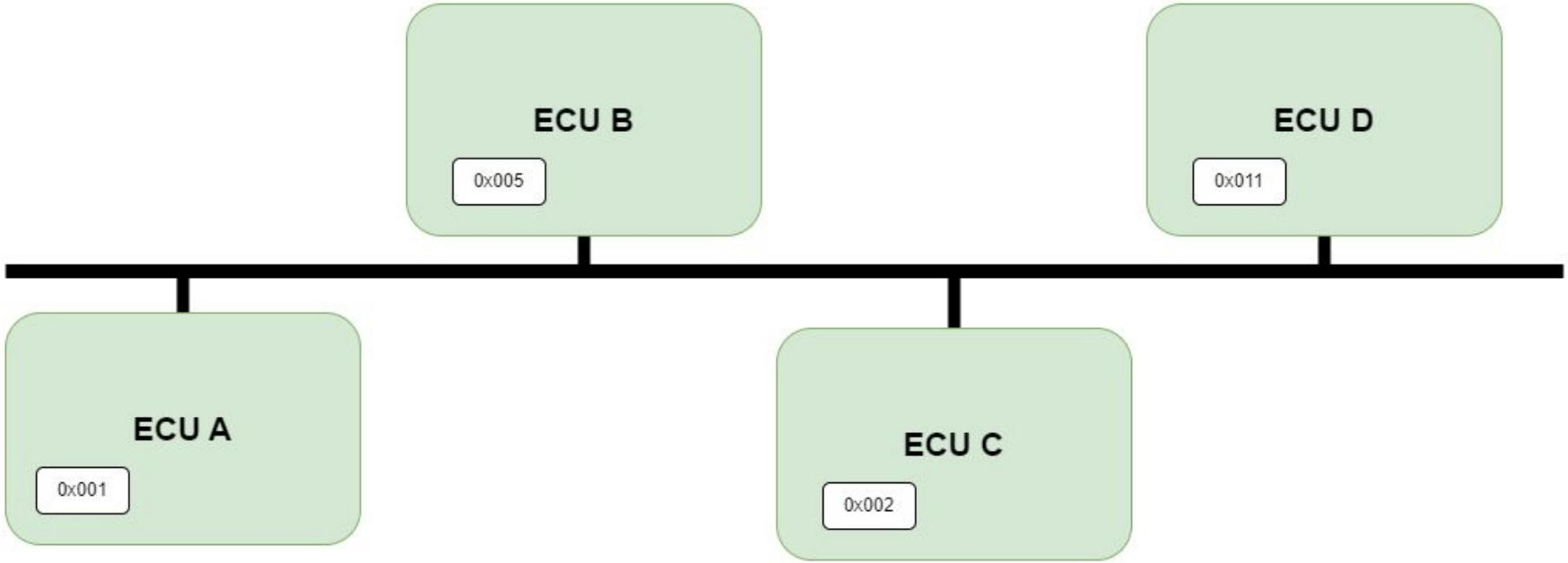


Figure 3: Message Authentication and Freshness Verification

https://www.autosar.org/fileadmin/standards/R4-3/CP/AUTOSAR_SWS_SecureOnboardCommunication.pdf


ECU B
0x005
ECU D
0x011
ECU A
0x001
ECU C
0x002

Diagnostic & Calibration Defenses

- UDS Strong Security Auth
- UDS Access Control Roles
- UDS Service Removal (unsafe SIDs)
- Removing XCP/CCP Support in Prod
- CAL File Integrity/Auth

- Service 29 Based Authentication with asymmetric crypto authentication
- Service 27 with asymmetric crypto authentication
- No more weak XOR or addition!

Diagnostic & Calibration Defenses

UDS Strong Security Auth

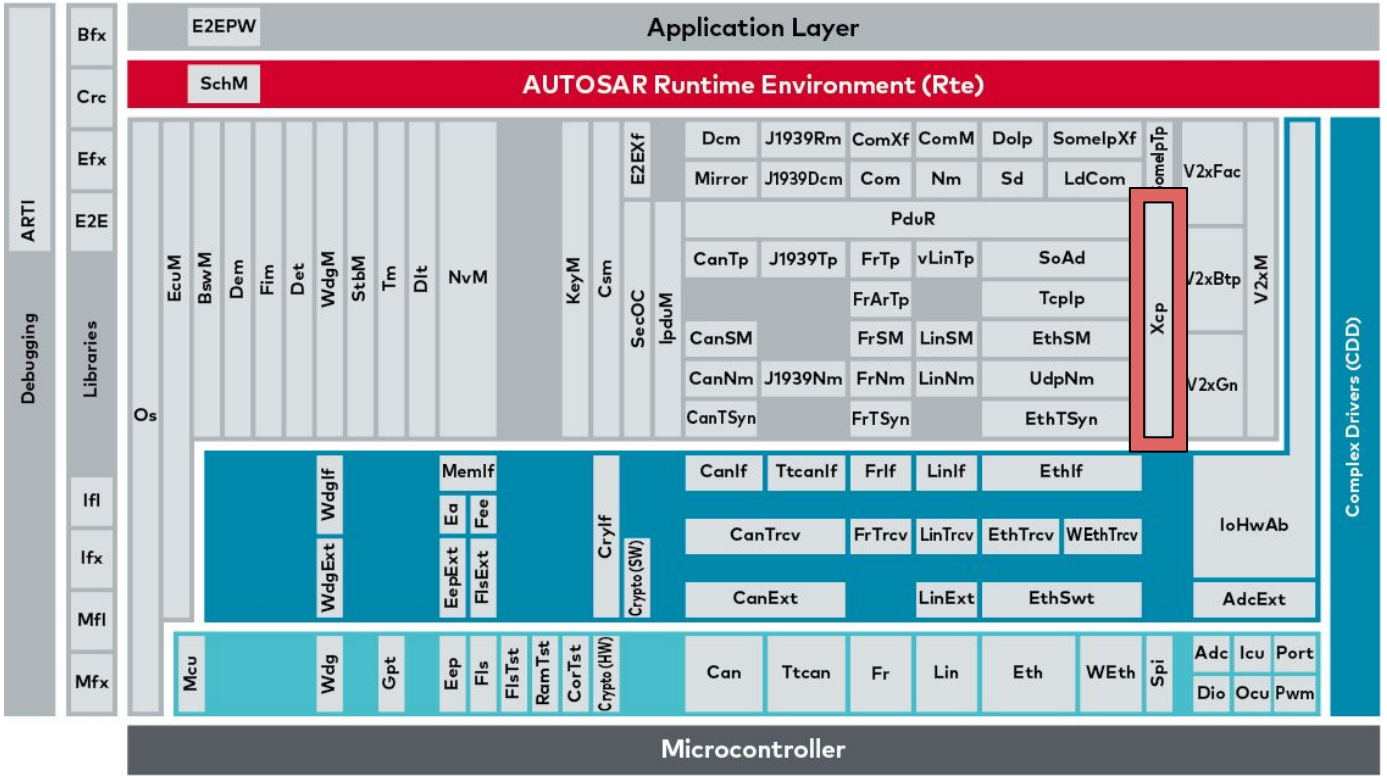
UDS Access Control Roles

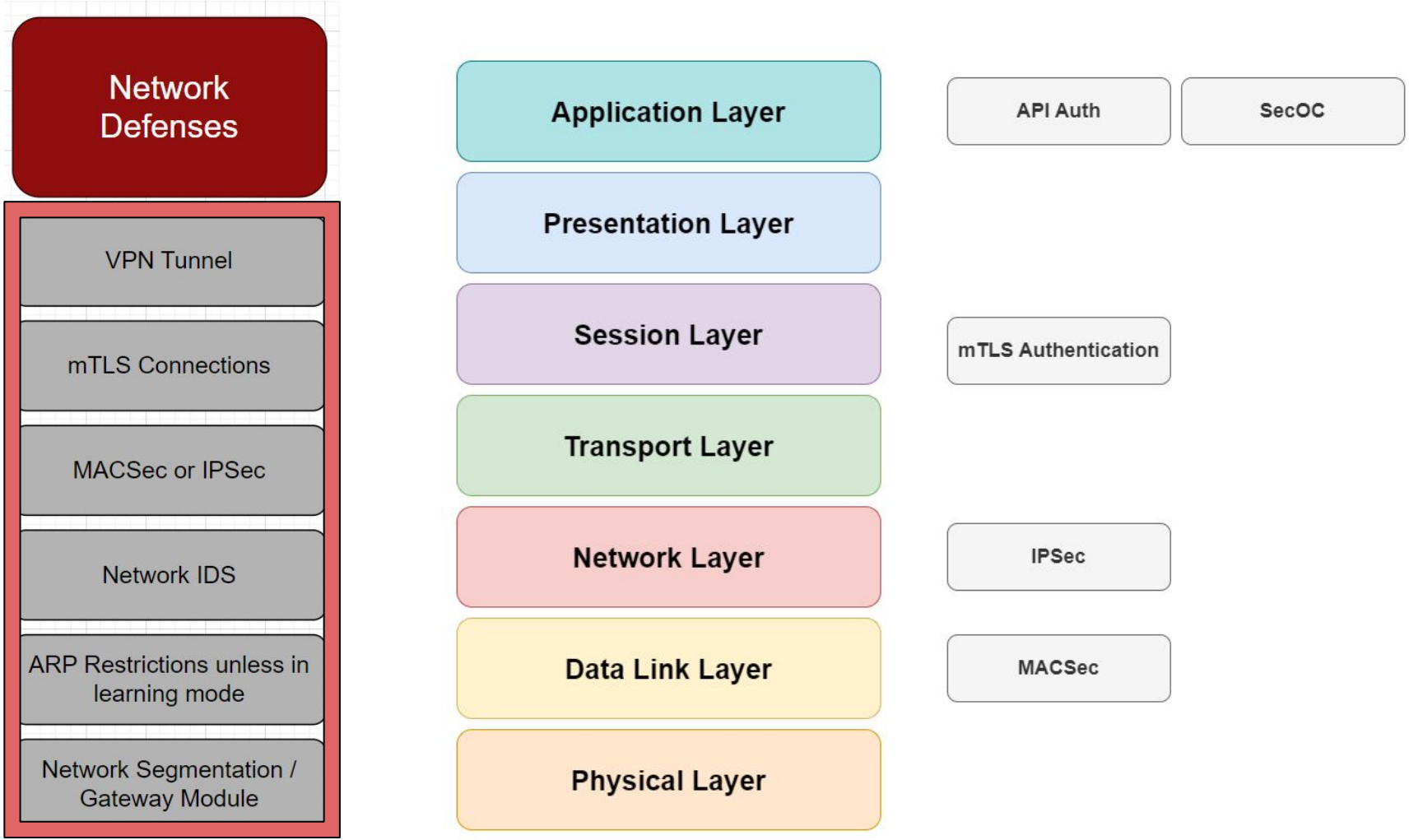
UDS Service Removal (unsafe SIDs)

Removing XCP/CCP Support in Prod

CAL File Integrity/Auth

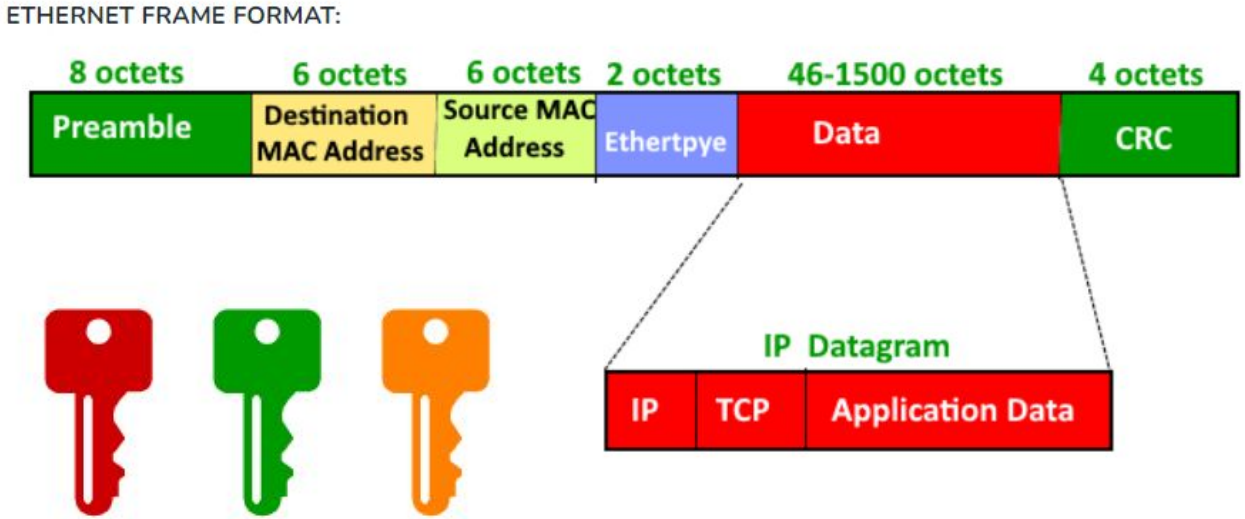
- Service 23 - Read Memory By Address
- Service 3D - Write Memory By Address
- Service 35 - Request Upload




Network Defenses
VPN Tunnel
mTLS Connections
MACSec or IPSec
Network IDS
ARP Restrictions unless in learning mode
Network Segmentation / Gateway Module
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
API Auth
SecOC
mTLS Authentication
IPSec
MACSec

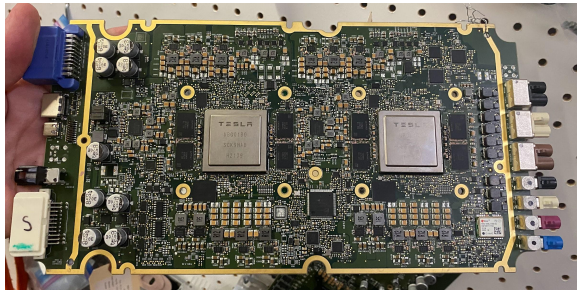
Network Defenses

- VPN Tunnel
- mTLS Connections
- MACSec or IPSec
- Network IDS
- ARP Restrictions unless in learning mode
- Network Segmentation / Gateway Module



https://www.geeksforgeeks.org/gate-gate-it-2006-question-19/#

In Summary



Hardened ECUs

Hardened Vehicle Networks

Thank you - Any Questions?

Application Defenses	Diagnostics & Calibration Defenses	Network Defenses
Operating System Defenses	Filesystem Defenses	Middleware Defenses
Hardware Defenses	Crypto Defenses	Firmware Defenses

Thank you to my Filipino and Singaporean friends at the Car Hacking Village in ROOTCON!