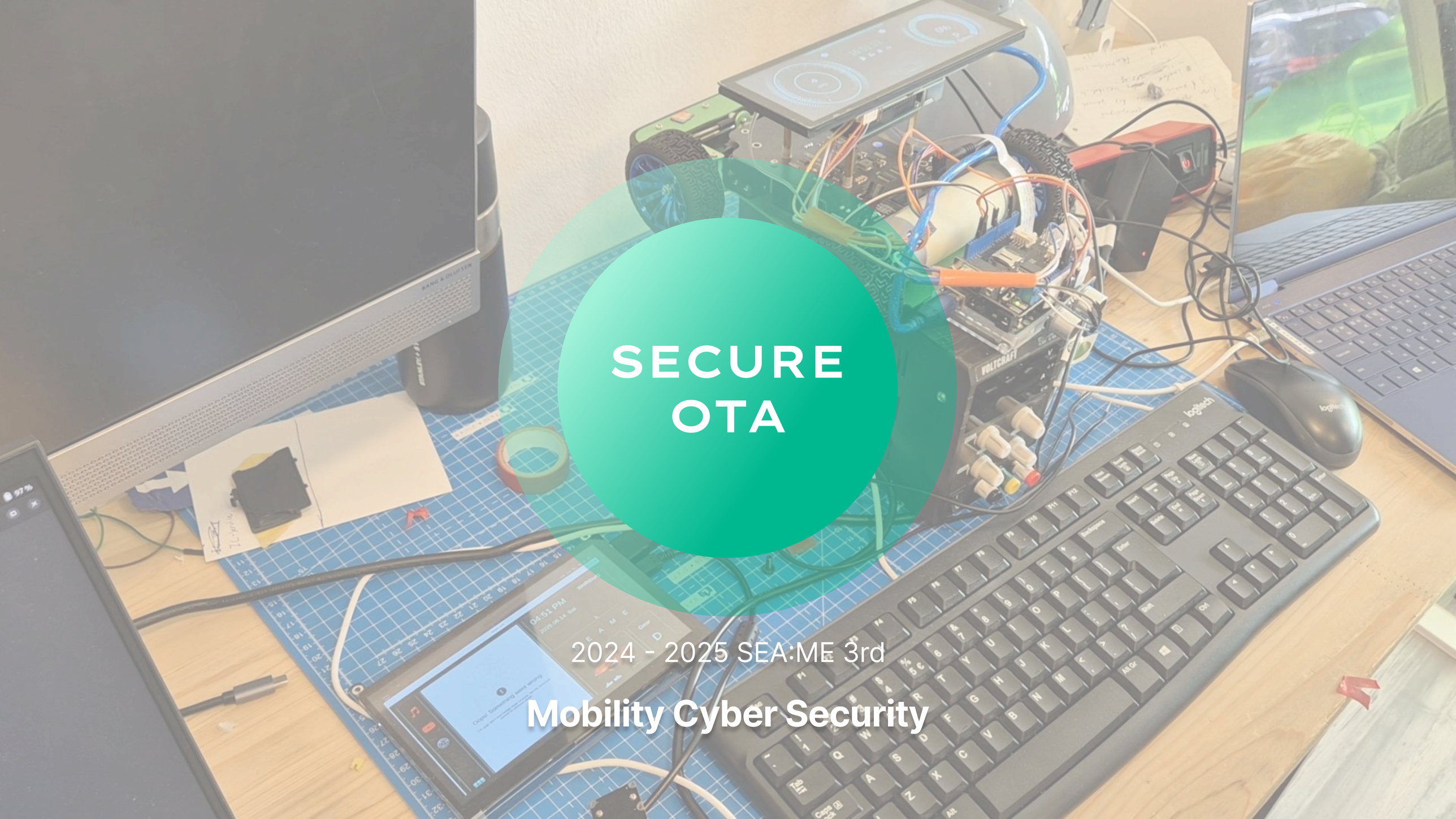
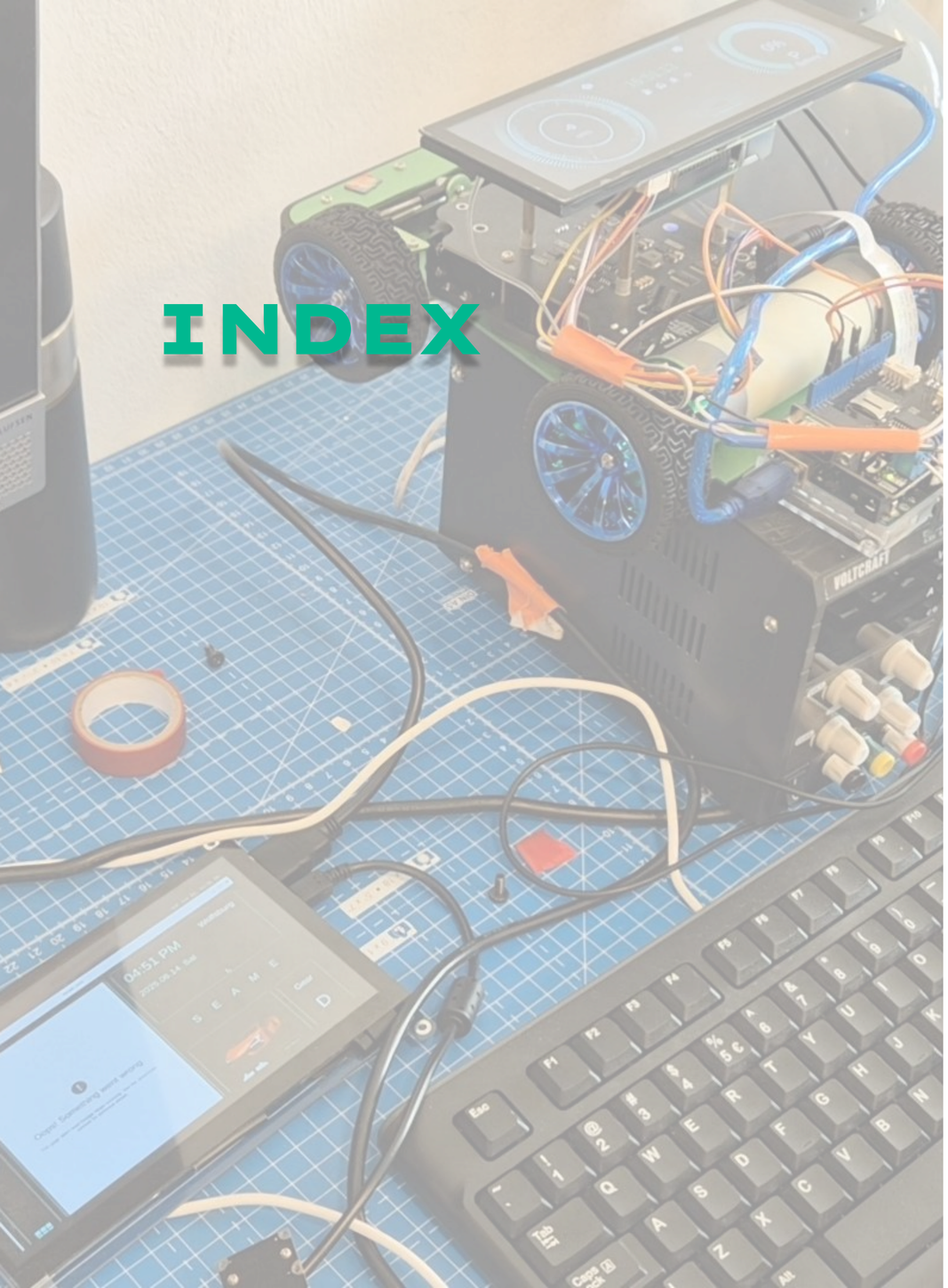

SECURE
OTA
2024 - 2025 SEA:ME 3rd
Mobility Cyber Security



INDEX

Members

Hanbin Yeo

Architecture
Network
Security
UX/UI Design

Jangwoon Park

Architecture
Network
Yocto

Kunho Park

Yocto
security
docker

Timeline

Feb 2025

Sprint 1
- Planning and Preparation
- Systems Architecture and Desgin

Sprint 2
- Develop Download Process

Mar 2025

Sprint 3
- Develop Installation Process

Sprint 4
- Develop Activation Process

Apr 2025

Sprint 5
- Secure system Architecture
- Modify Download Process based on Uptane

Sprint 6
- Apply Security Method

May 2025

Sprint 7 & 8
- Make Attack Scenarios
- Testing and Debugging
- Pilot/Proof of Concept Deployment

Today

Final Presentation

MileStone 1. Basic OTA

MileStone 2. Secure OTA

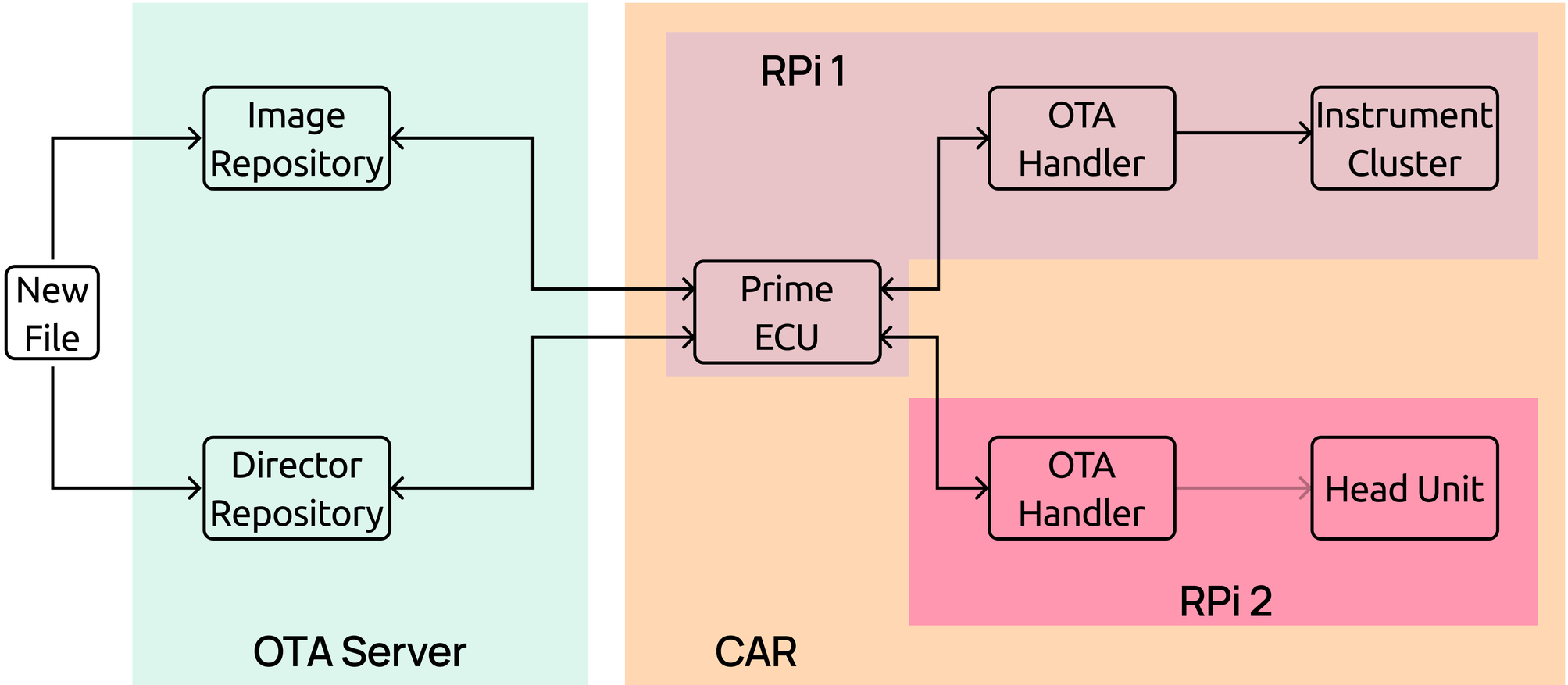
Over-The-Air(OTA):
Beyond Smartphone

What is Vehicle OTA?

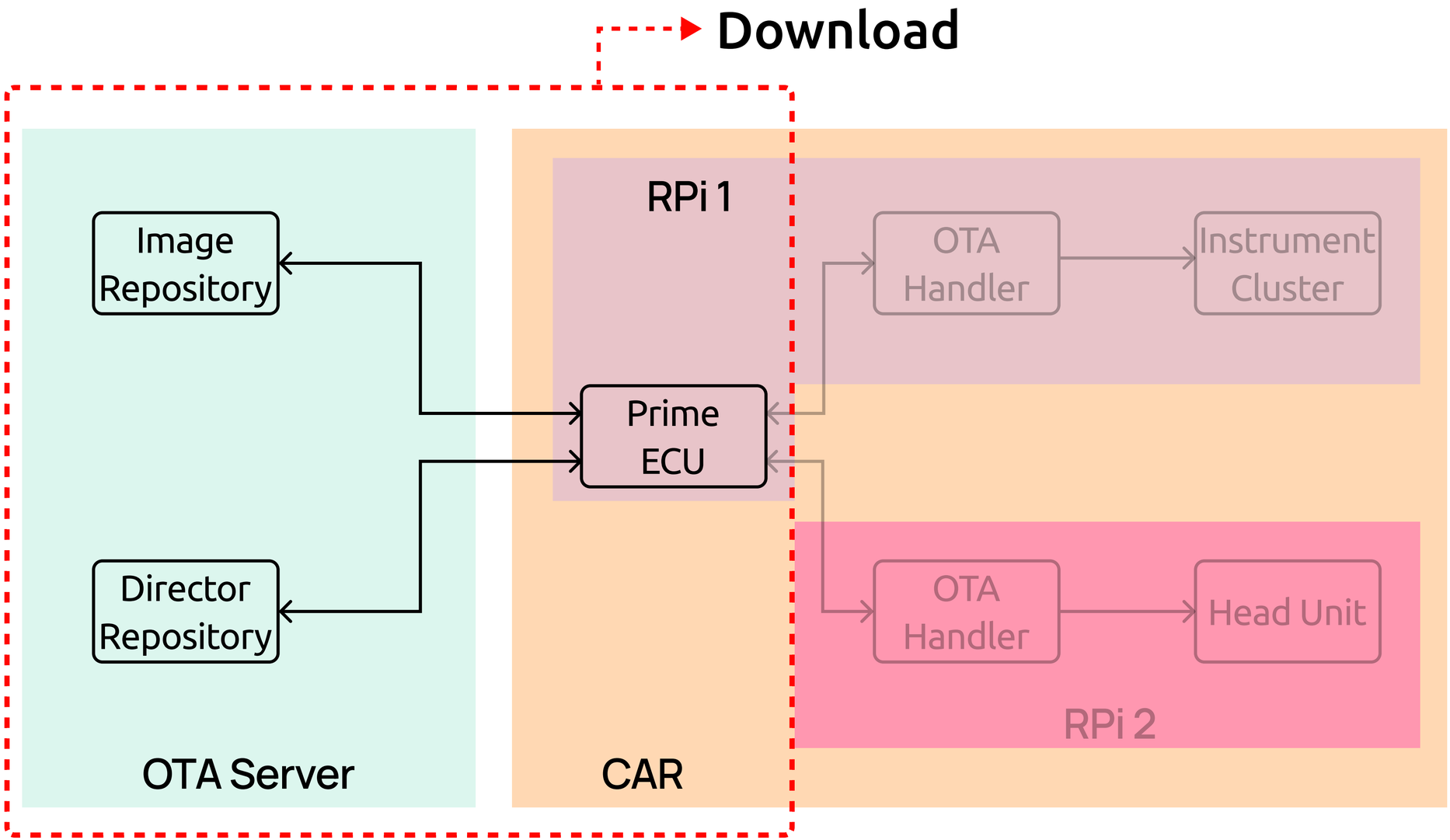
Why is Vehicle OTA Different from Phone Software?

- Safety Criticality
- System Complexity
- Cybersecurity Imperative
- Rollback & Redundancy
- Regulatory Compliance

Architecture



Download

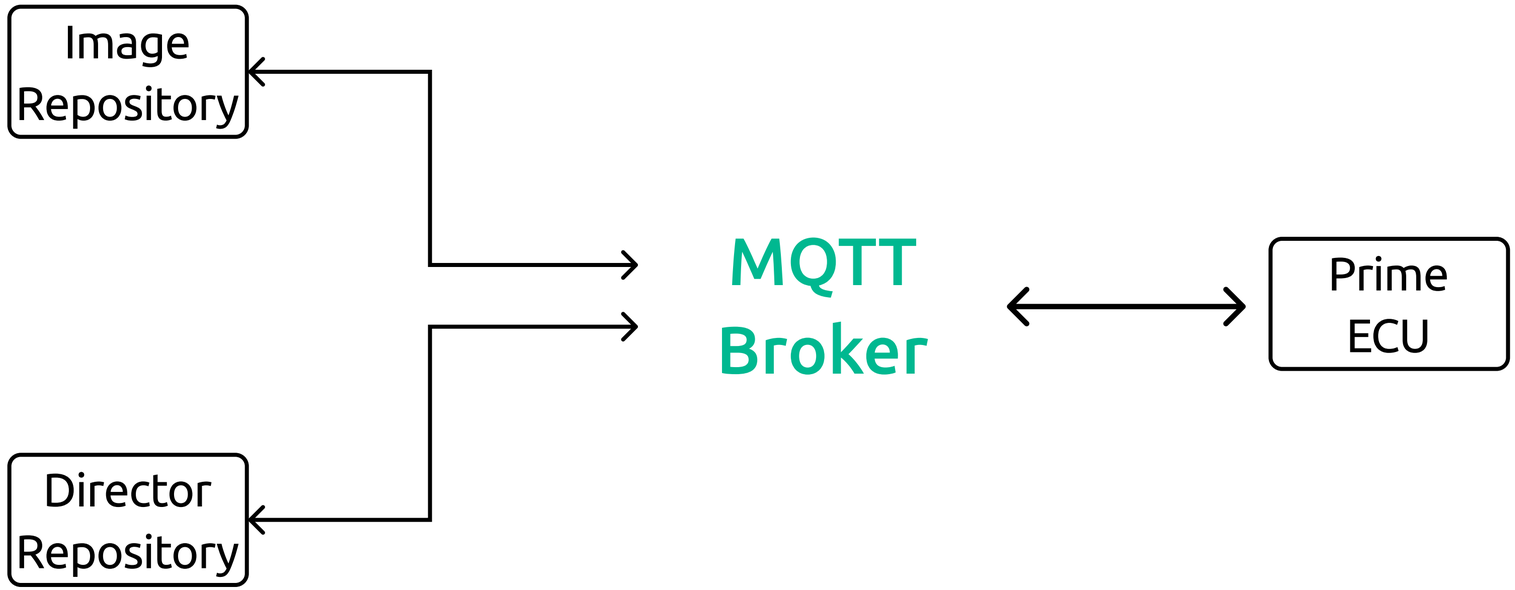

Download
RPi 1
Image Repository
Director Repository
Prime ECU
OTA Handler
Instrument Cluster
OTA Handler
Head Unit
RPi 2
OTA Server
CAR

Uptane Frame work

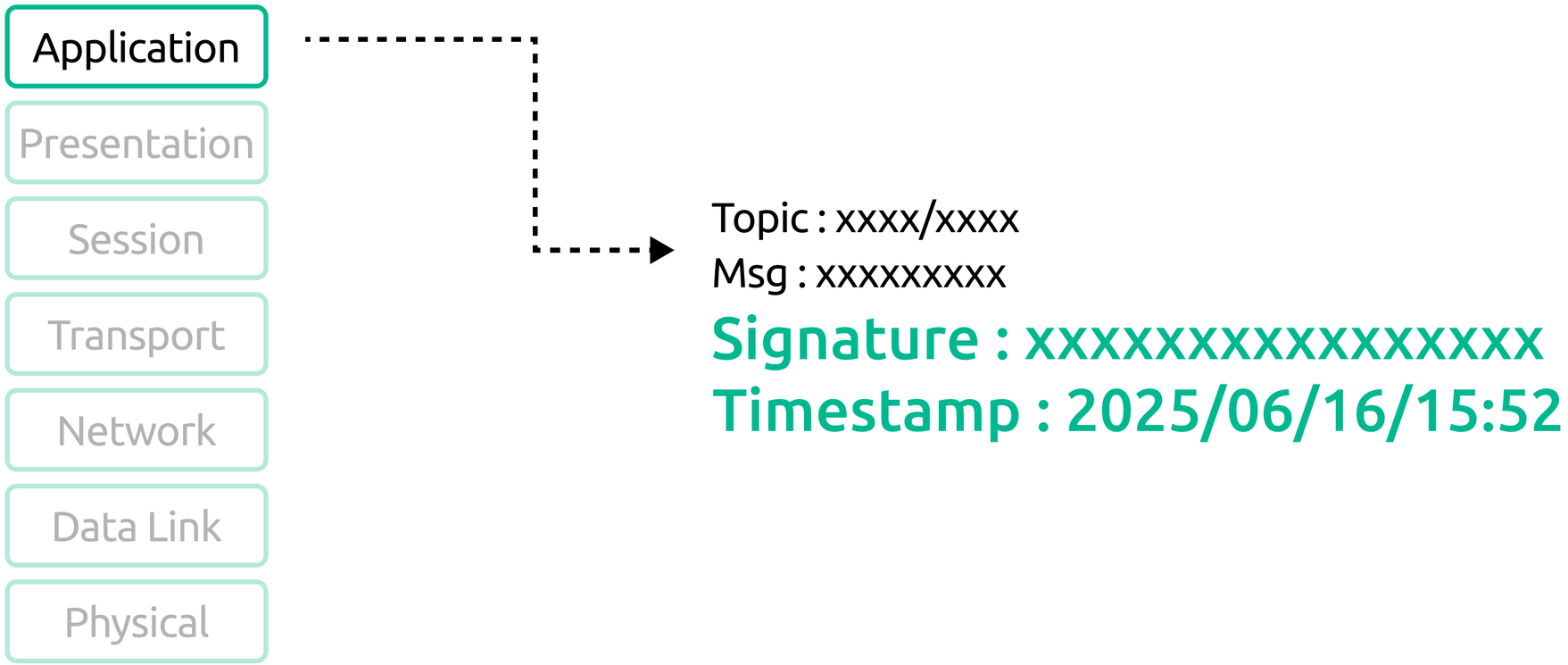
Uptane 

- Car OTA Update Framework
- Separation of trust
- Minimizes the risk

Update via MQTT



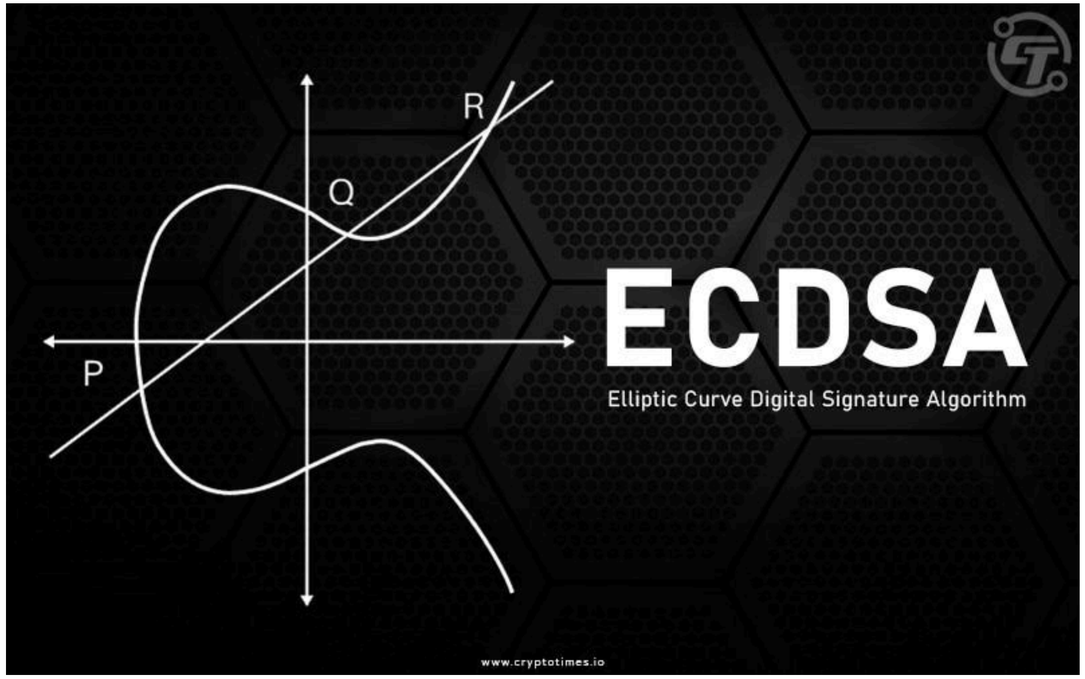
Signature & Timestamp



Signature - ECDSA

ECDSA

(Elliptic Curve Digital Signature Algorithm)

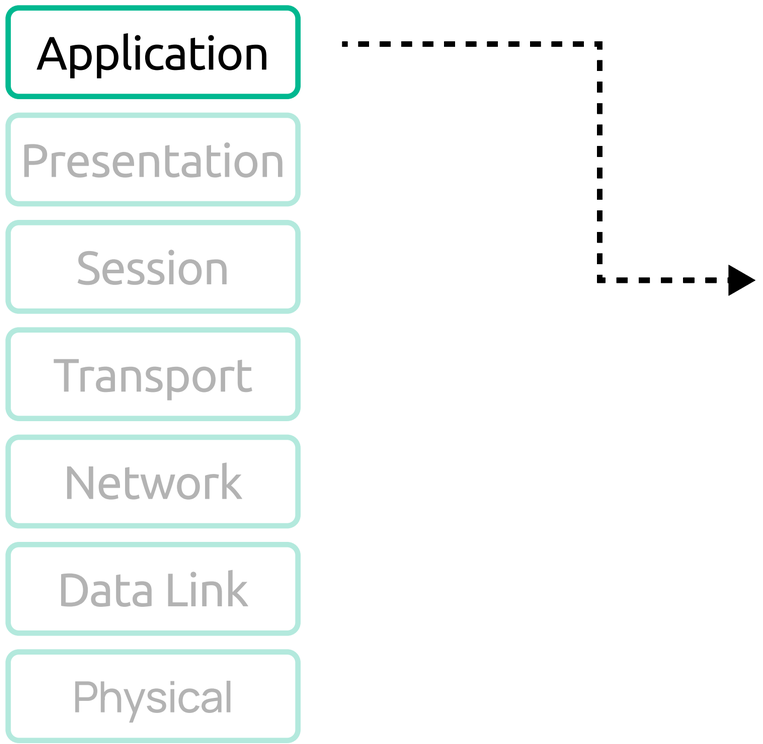


ECDSA vs RSA

RSA

ECDSA		RSA
384	Key Length	7680
936	Key Generation	0.4
904	Sign	12
491	Verify	1770

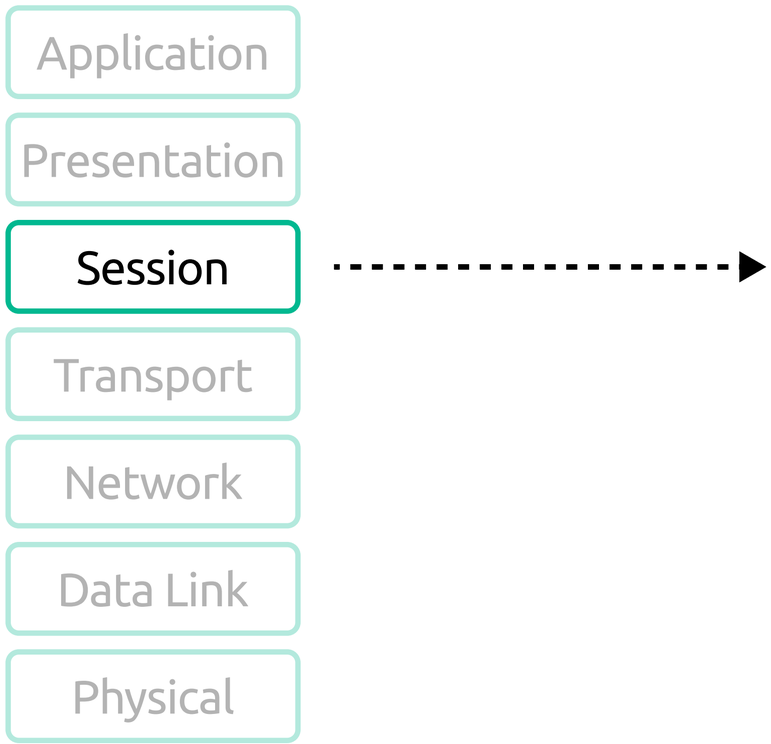
Timestamp



Topic : xxxx/xxxx
Msg : xxxxxxxxx
Signature : xxxxxxxxxxxxxxxx

Timestamp : 2025/06/16/15:52

TLS

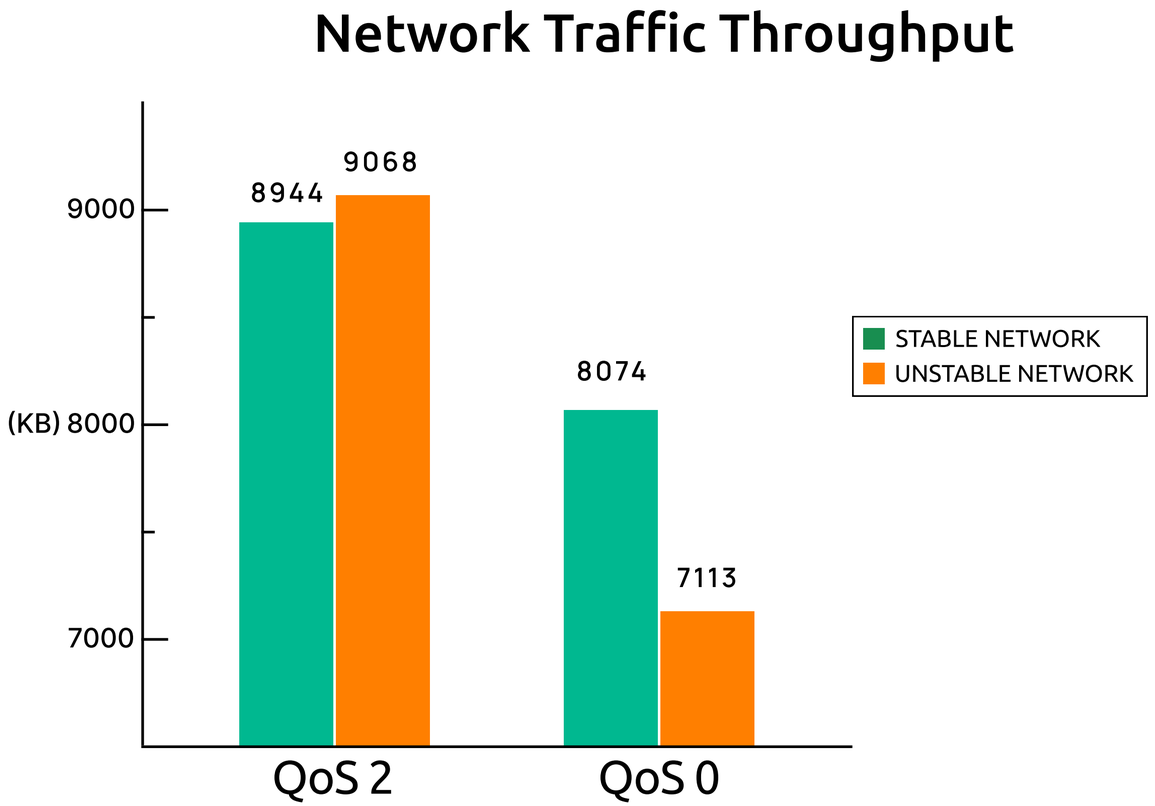


TLS

Topic : xxxx/xxxx
Msg : xxxxxxxxx
signature : xxxxxxxxxxxxxxxx
Timestamp : 2025/06/16/15:52

MQTT QoS Setting

- QoS 0 - At Most Once
- QoS 1 - At Least Once
- QoS 2 - Exactly Once



MQTT QoS Setting

QoS 0 - At Most Once

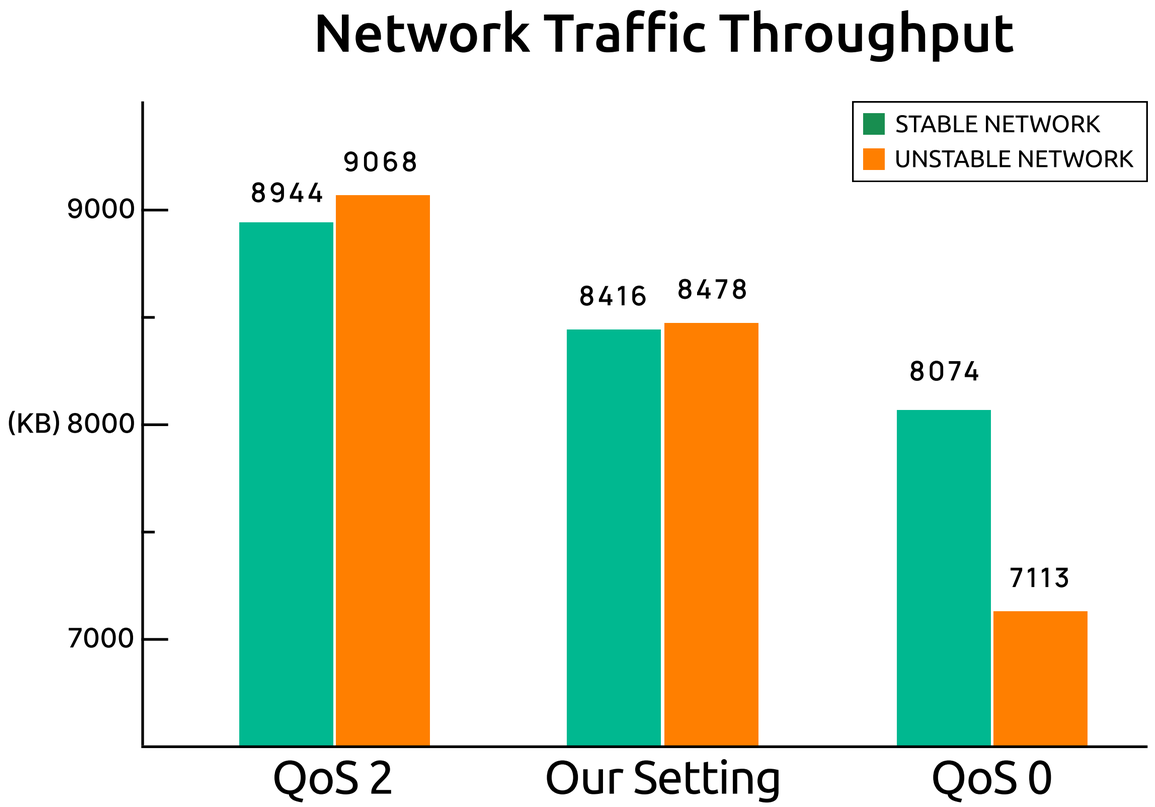
- Current version state

QoS 1 - At Least Once

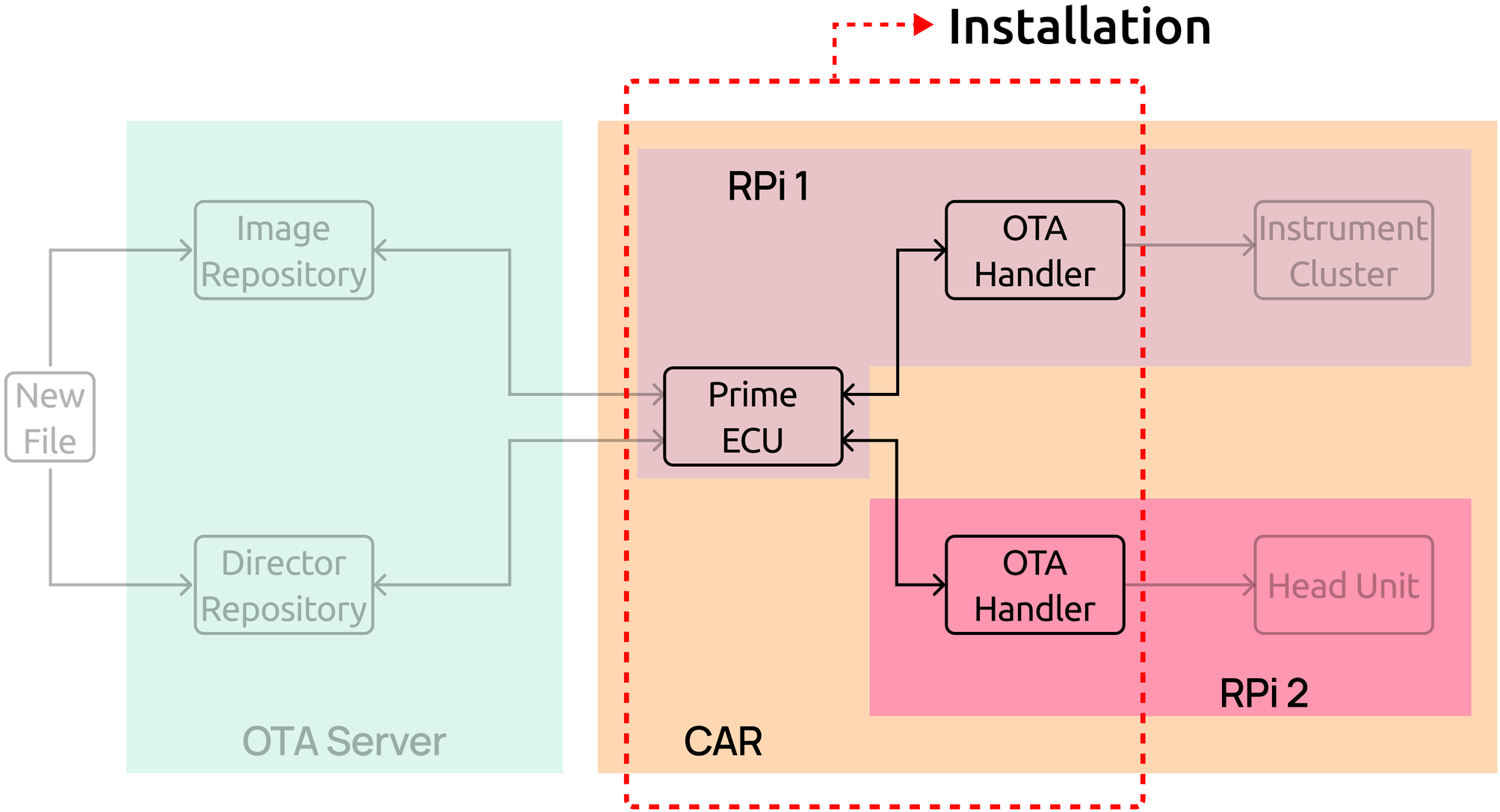
- Update meta data
- Request meta data

QoS 2 - Exactly Once

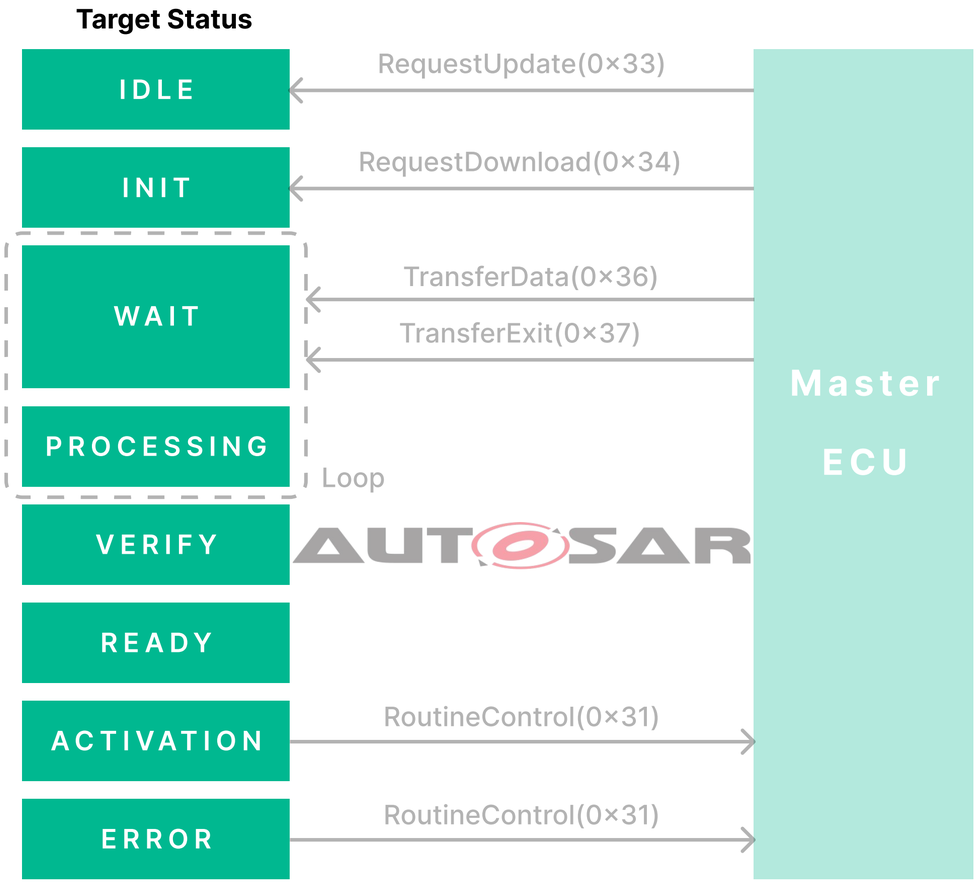
- Download URL

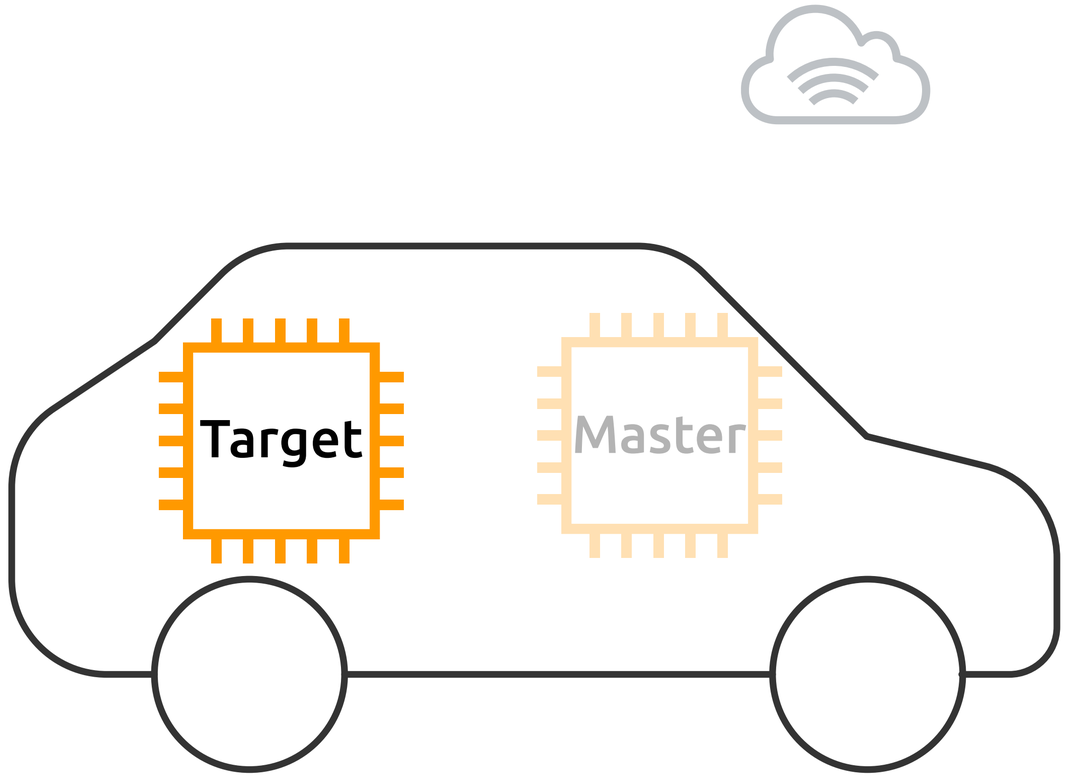


Installation

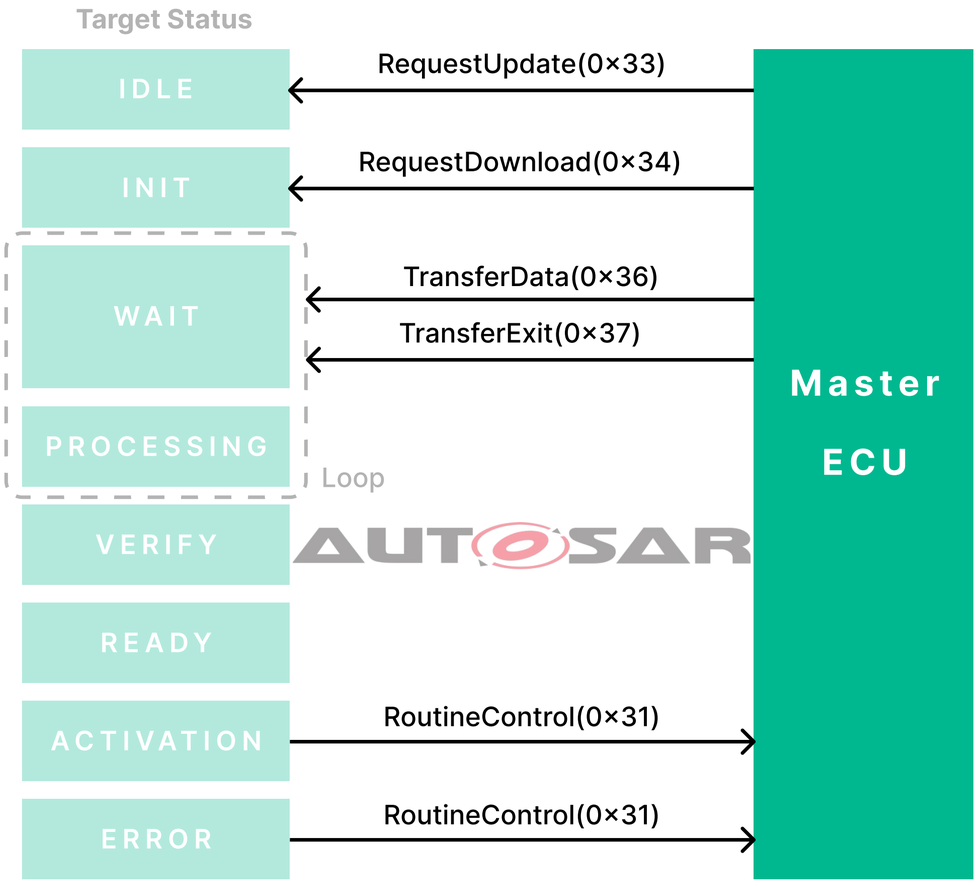


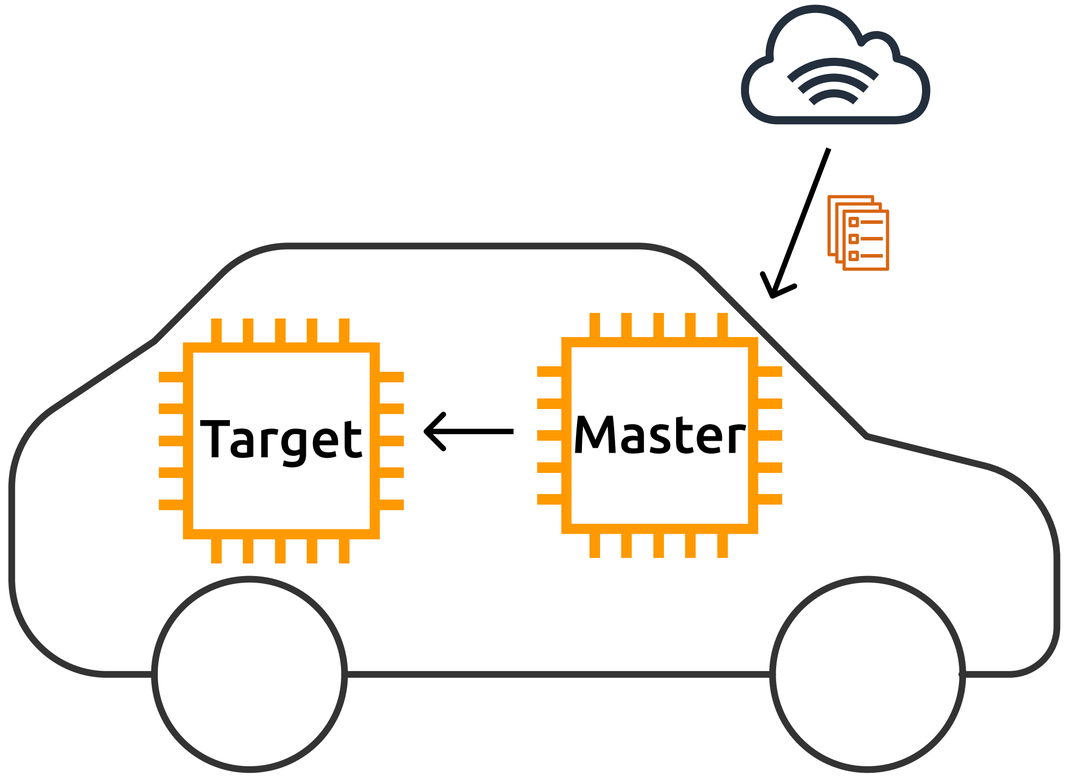
Installation - Process



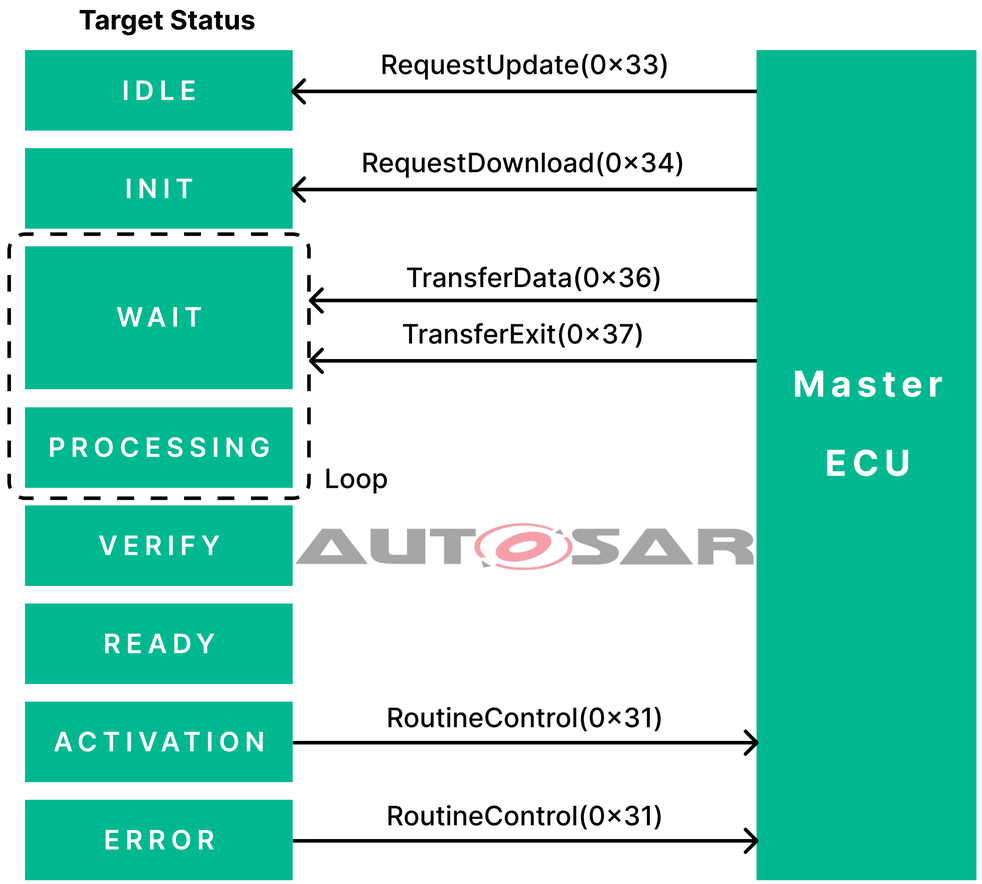


Installation - Process





Installation - Process



Payload Frame based on UDS protocol

Request

Service Identifier	Sub Function	Request Data	Padding
1 Byte	1 Byte	400 KB	

Response

Positive Response ID = Service Identifier + 0×30
Negative Response ID = 0×7F

Positive

Positive Response ID	Padding
1 Byte	400 KB

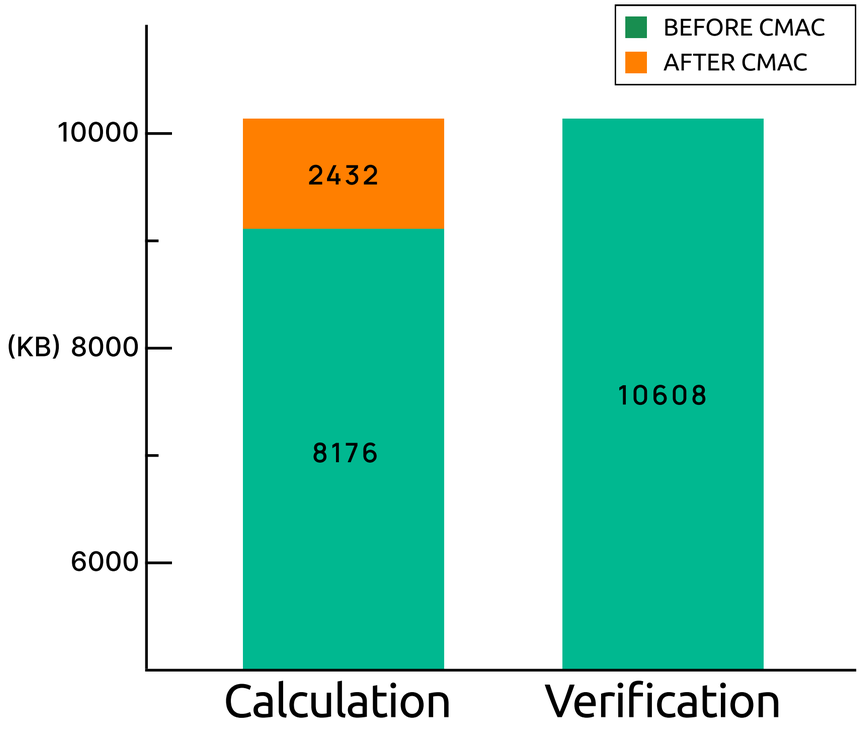
Negative

Negative Response ID	Rejected SID	Padding
1 Byte	1 Byte	400 KB

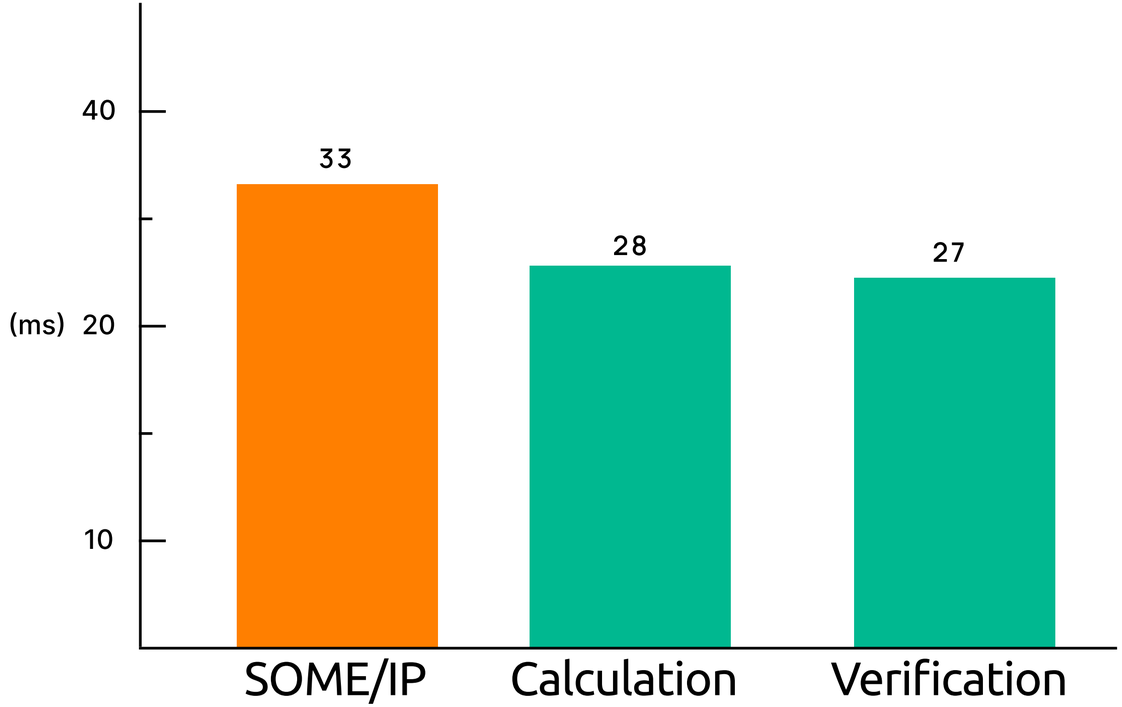
Installation - Verification

AES-CMAC

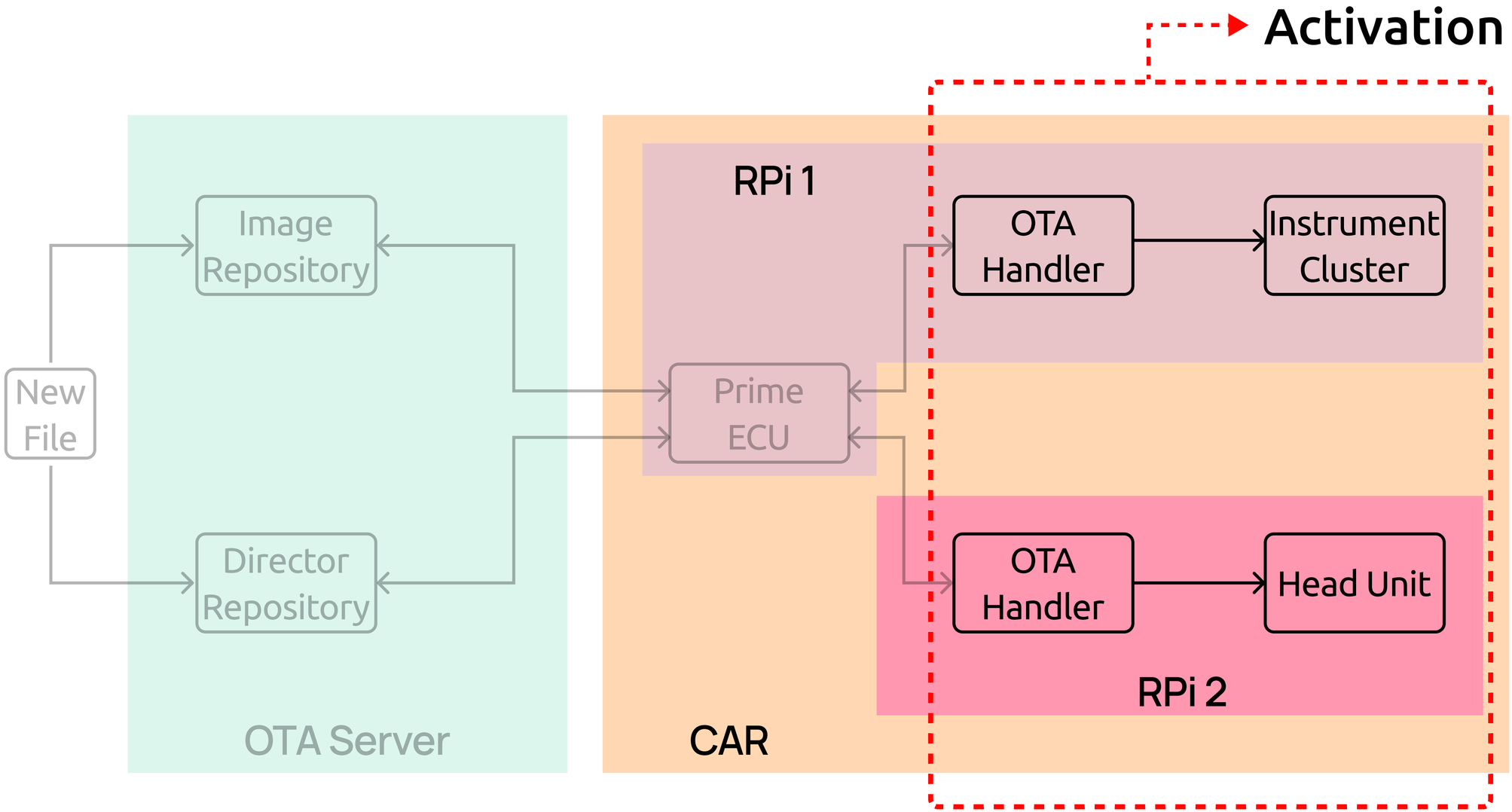
Memory Usage



Duration



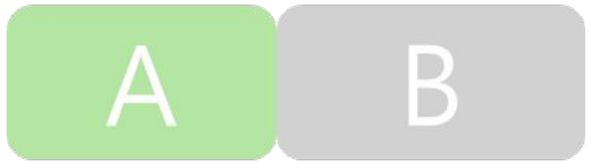
Architecture



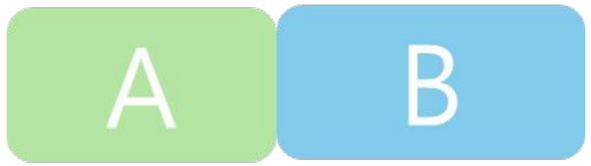
Activation - A/B Updates

Definition & Process

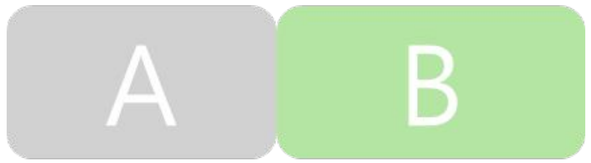
- Two identical system partitions (A and B)



- New software installs on inactive partition



- Partitions switch roles on success



Enhanced Reliability

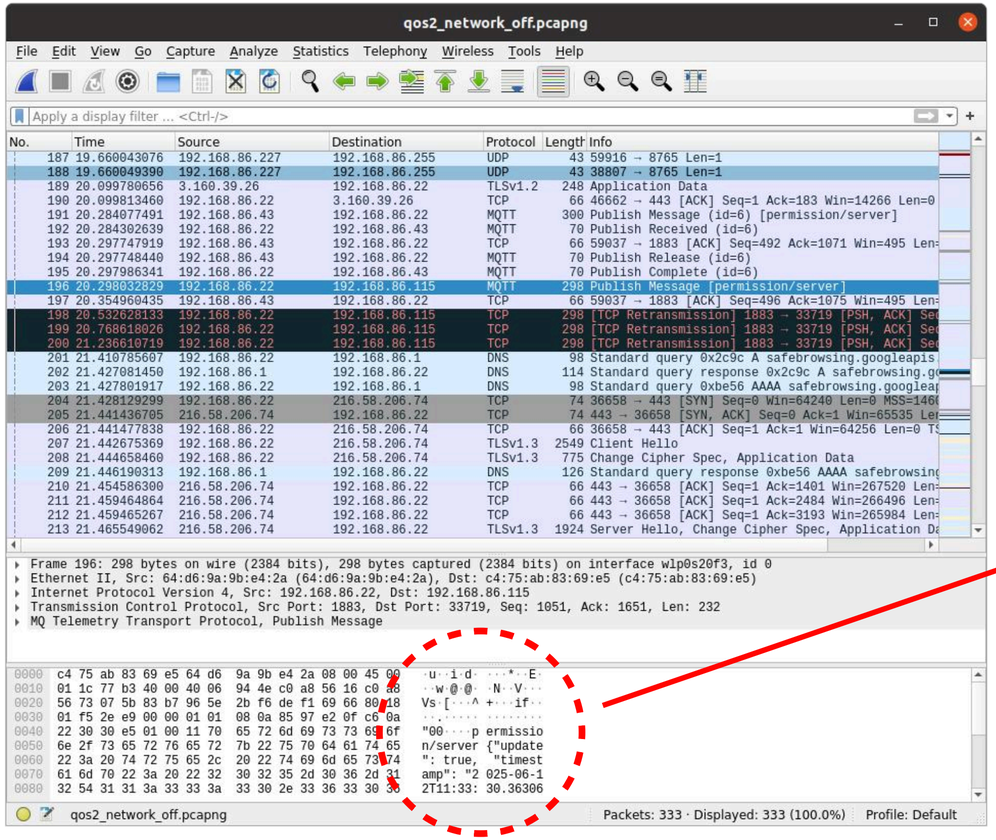
Seamless revert to previous version if update fails

Improved User Experience

Minimal interruption, vehicle stays operational

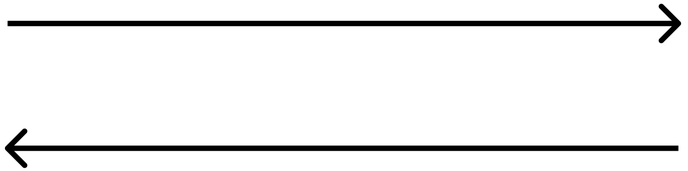
Attack Scenario 1 - Vulnerability

Attack Scenario 1 - Vulnerability



ATT 1 - ARP Spoofing

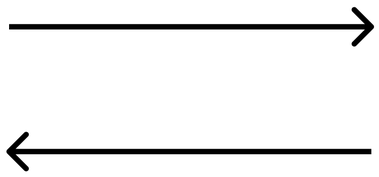
192.168.86.37



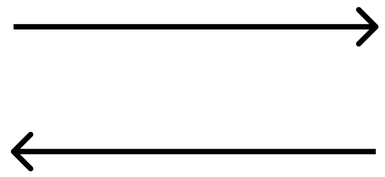
192.168.86.43

ATT 1 - ARP Spoofing

192.168.86.37



192.168.86.22



192.168.86.43

ATT 1 - DNS Redirection

192.168.86.37

192.168.86.22

REQUEST
http://192.168.86.37

GET
http://192.168.86.22

192.168.86.43

ATT 1 - How to protect

- TLS
- HSTS(HTTP Strict Transport Security)
- Digital Signature
- Periodical Update Process

ATT 2 - Original Update Scenario

192.168.86.37

192.168.86.43

Version : 2.0.0

2️⃣

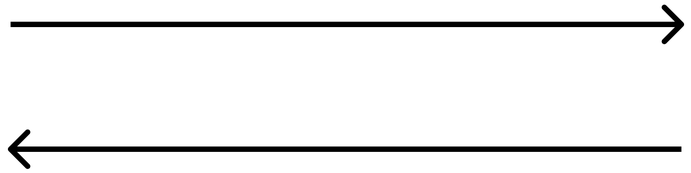
Version : 1.0.0

1️⃣

ATT 2 - Original Update Scenario

192.168.86.37

Version : 2.0.0



192.168.86.43

Version : 1.0.0 → 2.0.0

2️⃣

ATT 2 - Precondition

If attacker knows...

- Broker & Client IP address
- TLS certification
- Update Sequence

ATT 2 - Capture Message

192.168.86.37

Version : 2.0.0

192.168.86.22

Version : 2.0.0

2️⃣

192.168.86.43

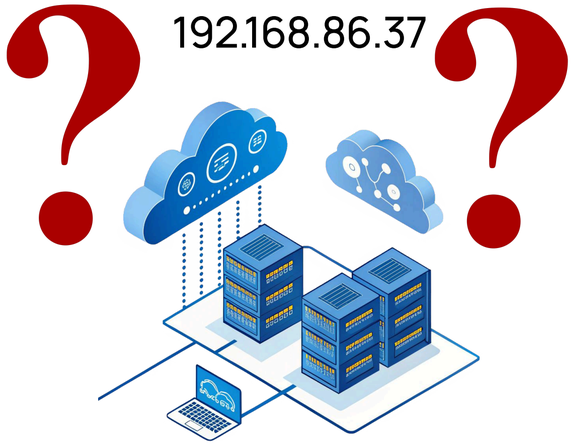
Version : 1.0.0 → 2.0.0

2️⃣

ATT 2 - Replay attack

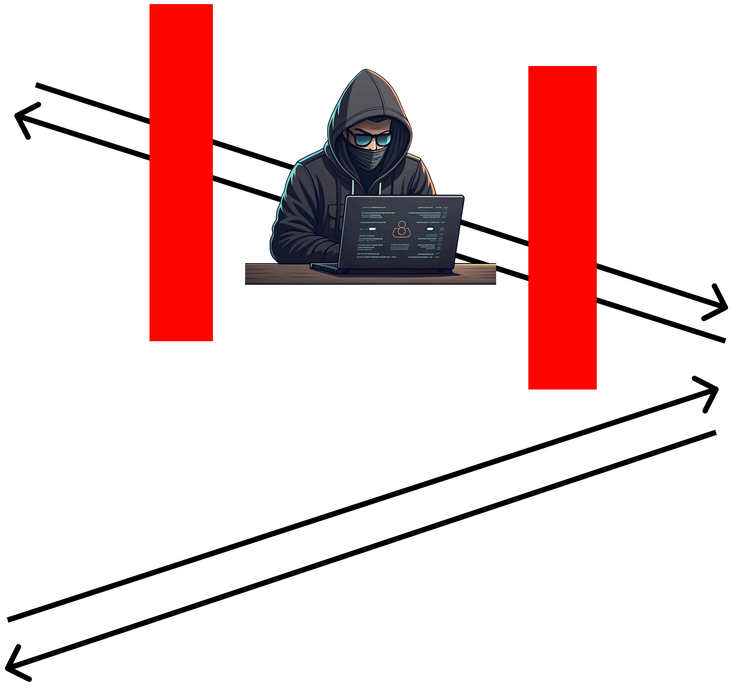
Find some vulnerability in version 2.0.0

ATT 2 - Replay attack



192.168.86.22

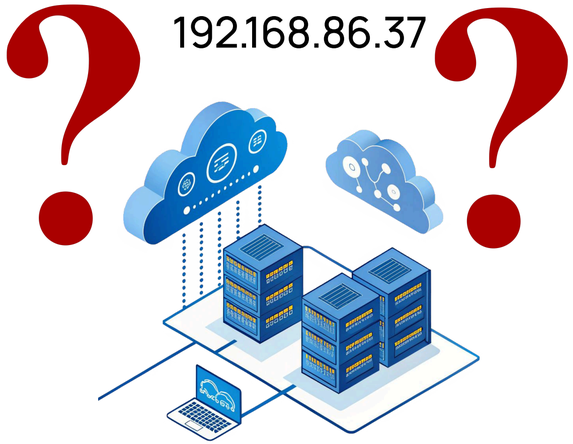
Version : 2.0.0



192.168.86.43

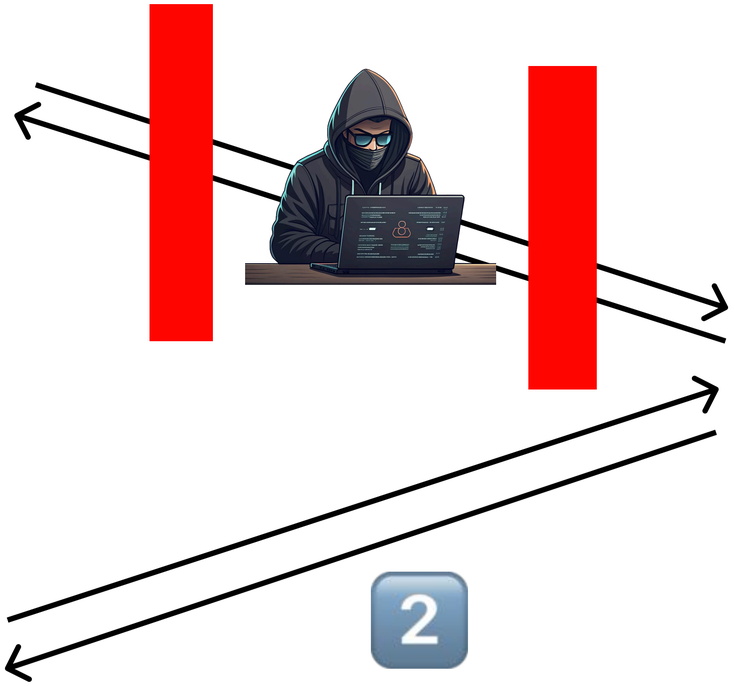
Version : 3.0.0

ATT 2 - Replay attack



192.168.86.22

Version : 2.0.0



2

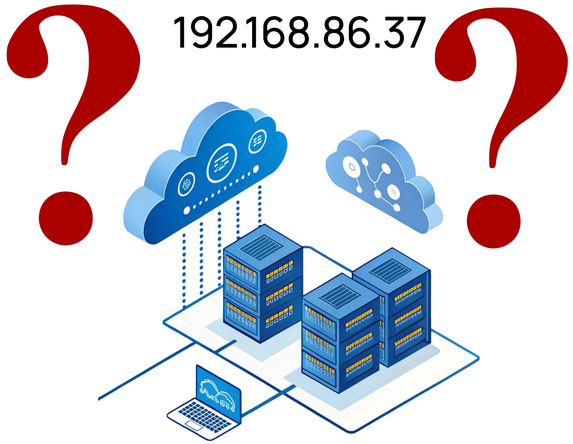
192.168.86.43

Version : 2.0.0

ATT 2 - Replay attack

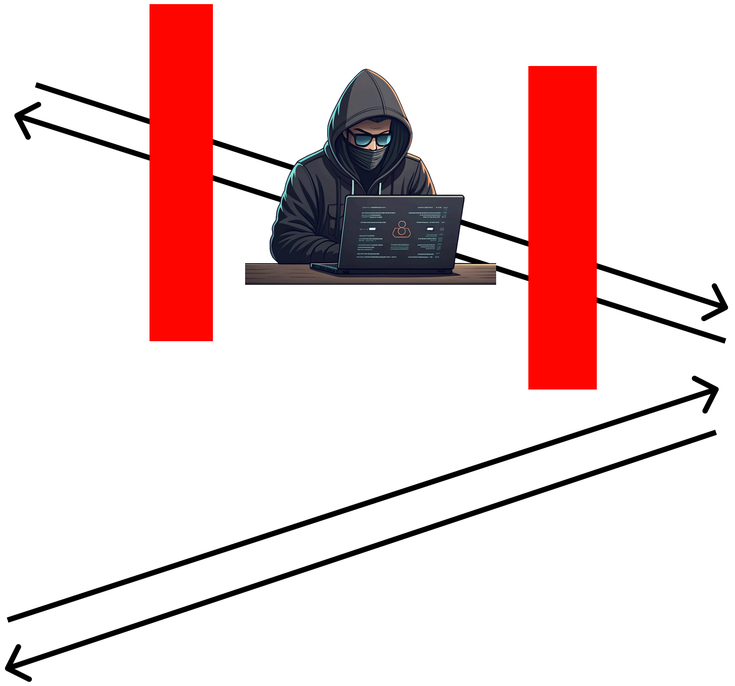
demo video

ATT 2 - How to protect



192.168.86.22

Version : 2.0.0

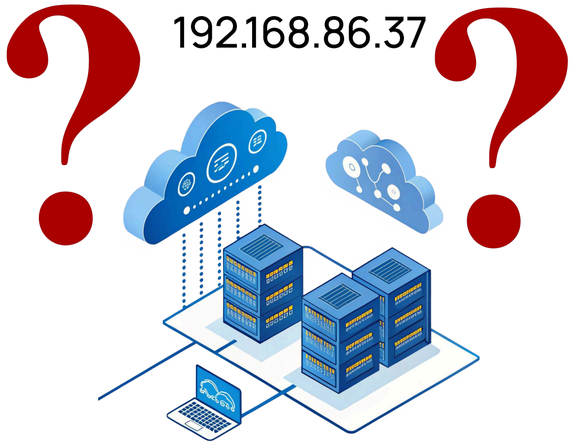


192.168.86.43

Version : 3.0.0

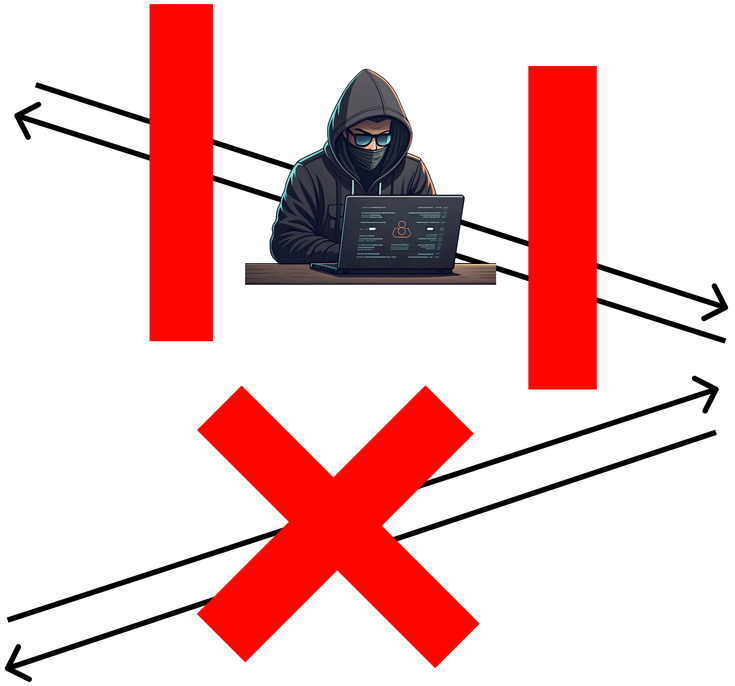
Timestamp

ATT 2 - How to protect



192.168.86.22

Version : 2.0.0



192.168.86.43

Version : 3.0.0

Timestamp

THANK YOU