CarPlay at Risk: Unveiling Security Threats of Third-Party Infotainment Adapters

Jun Yeon Won, Wenzhuo Wang, Keith Redmill, and Zhiqiang Lin

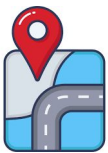
VehicleSec 2025

Modern Vehicles



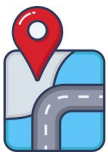
Modern Vehicles





Modern Vehicles

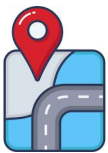






Modern Vehicles



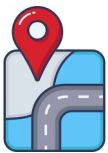






Modern Vehicles





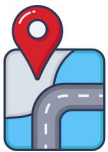






Modern Vehicles







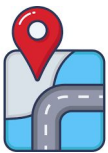






Modern Vehicles







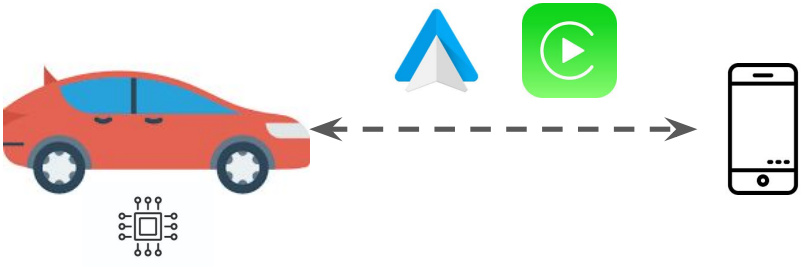




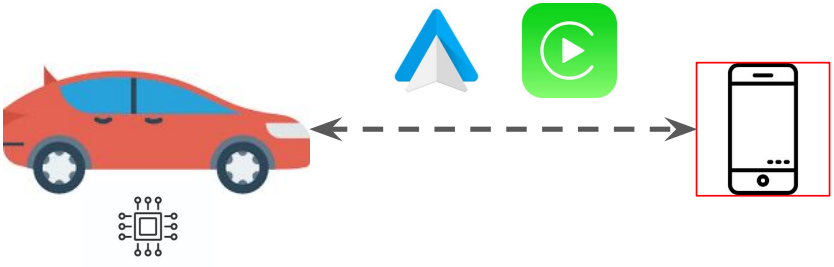




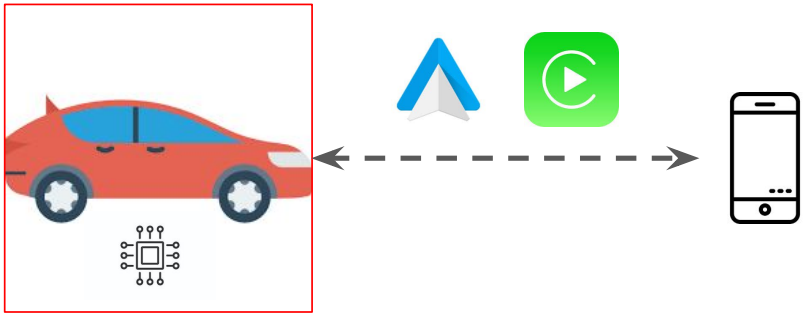
Apple CarPlay



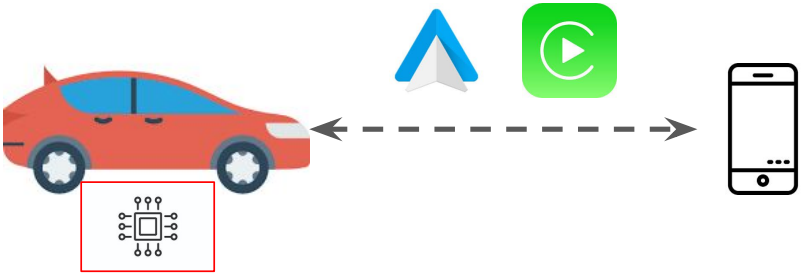
Apple CarPlay



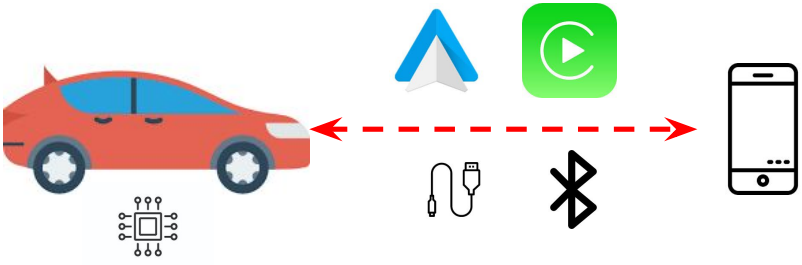
Apple CarPlay



Apple CarPlay



Apple CarPlay



Apple CarPlay



Apple CarPlay





Apple CarPlay



Apple CarPlay



In-Vehicle Adapters







CarPlay Adapter Video

CarPlay Adapter Video

Any Observations?

CarPlay Adapter Video

Any Observations?



CarPlay Adapter Video

Any Observations?





CarPlay Adapter Video

Any Observations?







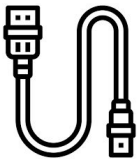
How and Why Does It Happen?

How and Why Does It Happen?



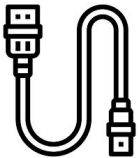
How and Why Does It Happen?





How and Why Does It Happen?

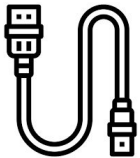






How and Why Does It Happen?



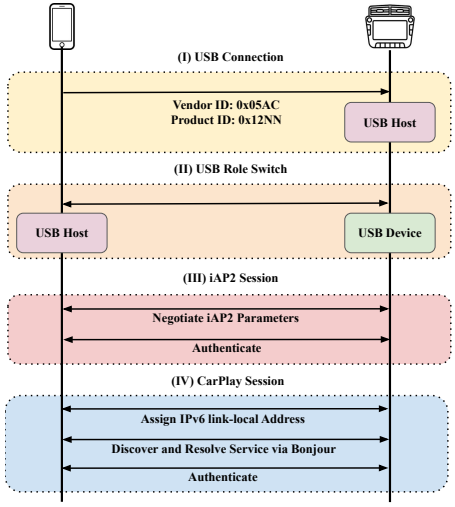




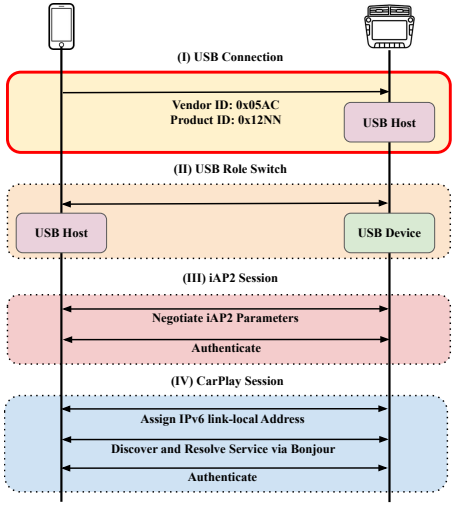


Document-based Analysis

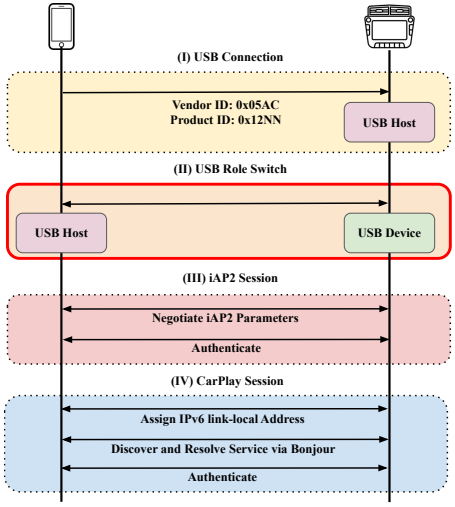
Document-based Analysis



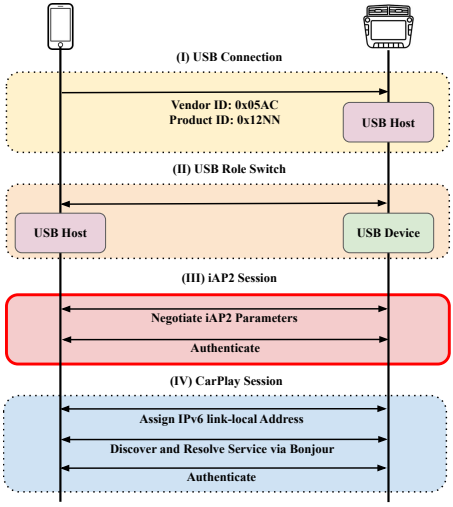
Document-based Analysis



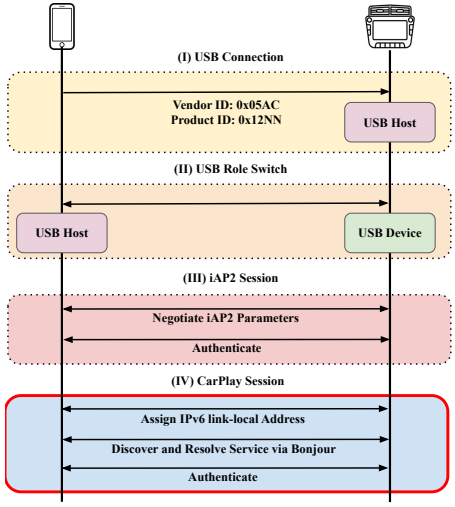
Document-based Analysis



Document-based Analysis



Document-based Analysis



USB Packet Analysis



USB Packet Analysis

USB role switch packets

Source	Destination	Packets
		First Request
IVI	Adapters	C0 53 00 00 00 00 04 00
		4-Byte Payload
Adapters	IVI	01 00 00 00
		Second Request
IVI	Adapters	40 51 01 00 00 00 00 00
		Disconnected
		Reconnected

USB Packet Analysis

Parameter negotiation and identification of USB packets

Source	Destination	Packets
		Handshake
IVI	Adapters	ff 55 02 00 ee 10
		Handshake
Adapters	IVI	ff 55 02 00 ee 10
		Parameters Negotiation
IVI	Adapters	ff 5a 00 1a 80 e8 00 00 25 01 40 20 00 03 e8 00 32 1e 14 01 00 02 02 01 01 49
		Parameters Negotiation
Adapters	IVI	ff 5a 00 1a c0 1d e8 00 c8 01 7f ff ff 03 e8 00 32 1e 14 01 00 02 02 01 01 2c
		Start Identification
Adapters	IVI	ff 5a 00 10 40 1e e8 01 50 40 40 00 06 1d 00 5d
		Information
IVI	Adapters	ff 5a 01 40 40 e9 1e 01 1e 40 40 01 36 1d 01 00 0b 00 00 53 6f 6e 61 74 61 00 00 08 00 01 44 4e 38 00 00 12 00 02 48 59 55 4e 44 41 49 20 4d 4f 42 49 53 00 00 11 00 03 32 38 63 66 30 38 61 62 36 33 33 62 00 00 18 00 04 44 4e 38 2e 55 53 41 2e 44 32 56 2e 30 30 31 2e 30 30 33 00 00 0d 00 ...
		Identification Accepted
Adapters	IVI	ff 5a 00 10 40 1f e9 01 4e 40 40 00 06 1d 02 5b

USB Packet Analysis

Authentication of USB packets

Source	Destination	Packets
		Request Authentication Certificate
Adapters	IVI	ff 5a 00 10 40 20 e9 01 4d 40 40 00 06 aa 00 d0
		Certificate
IVI	Adapters	ff 5a 03 a0 40 ea 20 01 b9 40 40 03 96 aa 01 03 90 00 00 30 82 03 88 06 09 2a 86 48 86 f7 0d 01 07 02 a0 82 03 79 30 82 03 75 02 01 01 31 00 30 0b 06 09 2a 86 48 86 f7 0d 01 07 01 a0 82 03 5d 30 82 03 59 30 82 02 41 a0 03 02 01 02 02 0f 22 22 aa 18 08 21 aa 04 aa 77 56 aa 58 16 51 30 0d ...
		Request Authentication Certificate Challenge Response
Adapters	IVI	ff 5a 00 28 40 21 ea 01 33 40 40 00 1e aa 02 00 18 00 00 79 70 4e d5 f2 dc 9c 7d 43 f3 54 ec 44 a4 c7 5b 01 4c de b7 49
		Response
IVI	Adapters	ff 5a 00 94 40 eb 21 01 c6 40 40 00 8a aa 03 00 84 00 00 3b 24 7a 19 40 6e 1c 52 f5 5d 3c 98 6b ed d8 30 ee fb 4b ed 3c 5e 58 7b 43 4f e8 de ba b2 c9 da 00 52 e6 ee e4 86 da 25 a7 e3 40 15 c8 41 6a 30 db cb d0 1a 4f d5 c4 aa 1f 76 cb 97 59 bc c0 d2 02 c8 c1 5f 48 0f d2 1a 8c e6 84 cc c5 96 83 c2 96 ee 7f 3e f2 01 03 78 21 f2 f9 86 17 64 b8 4e 7e 98 79 d8 60 ce 2f 48 f2 34 62 0e 40 b2 90 3c 9a 96 8e 0d 07 9b 7a a5 3a 1b c4 57 19 6d 83 7d 38
		Authentication Response
Adapters	IVI	ff 5a 00 10 40 22 eb 01 49 40 40 00 06 aa 05 cb

USB Packet Analysis

Summary

The adapter is sending and receiving packets that are almost identical, with the only differences being the challenge and response fields.

Adapter Log Analysis

Findings

Adapter Log Analysis

Findings

- Matched the packets to their corresponding protocol steps.

Adapter Log Analysis

Findings

- Matched the packets to their corresponding protocol steps.
- Identified diverse device addresses (e.g., Bluetooth address).

Adapter Log Analysis

Findings

- Matched the packets to their corresponding protocol steps.
- Identified diverse device addresses (e.g., Bluetooth address).
- Observed various functionalities that become available after the authentication process (e.g., location updater).

Adapter Log Analysis

Findings

- Matched the packets to their corresponding protocol steps.
- Identified diverse device addresses (e.g., Bluetooth address).
- Observed various functionalities that become available after the authentication process (e.g., location updater).
- Discovered information related to cryptographic keys.

Static Binary Analysis

Findings

Static Binary Analysis

Findings

- Identified cryptographic processes in use (e.g., ChaCha encryption).

Static Binary Analysis

Findings

- Identified cryptographic processes in use (e.g., ChaCha encryption).
- Detected the presence of MFi certificates.

Static Binary Analysis

Findings

- Identified cryptographic processes in use (e.g., ChaCha encryption).
- Detected the presence of MFi certificates.
- Analyzed three-byte differences between packets, attributing them to a counter and checksum.

Static Binary Analysis

Findings

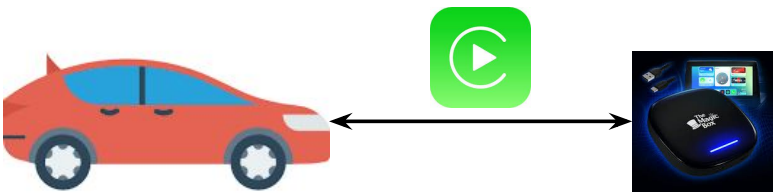
- Identified cryptographic processes in use (e.g., ChaCha encryption).
- Detected the presence of MFi certificates.
- Analyzed three-byte differences between packets, attributing them to a counter and checksum.
- Outlined the process of challenge and response.

Root Cause

How does the adapter utilize CarPlay?

Root Cause

How does the adapter utilize CarPlay?

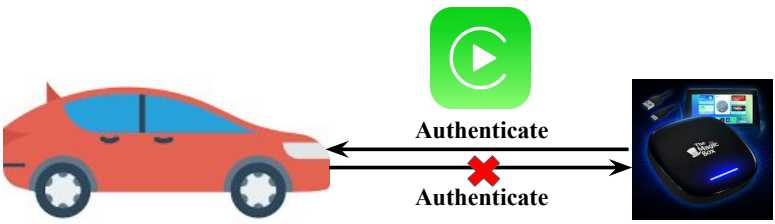


Root Cause

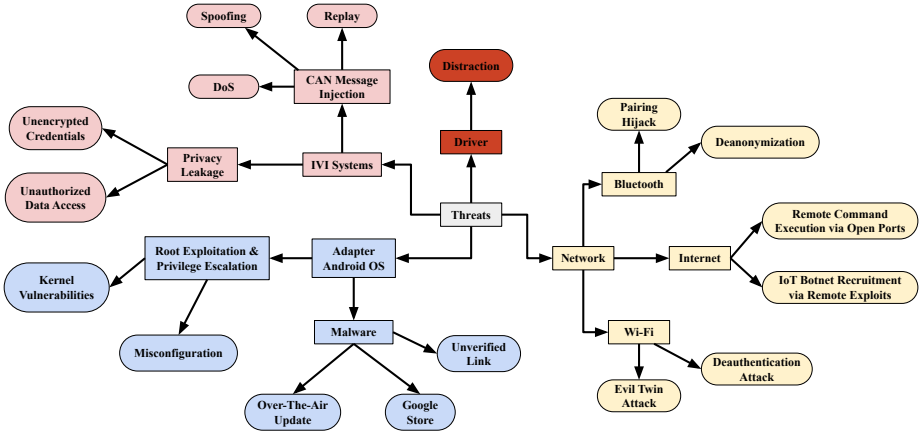
Why?

Root Cause

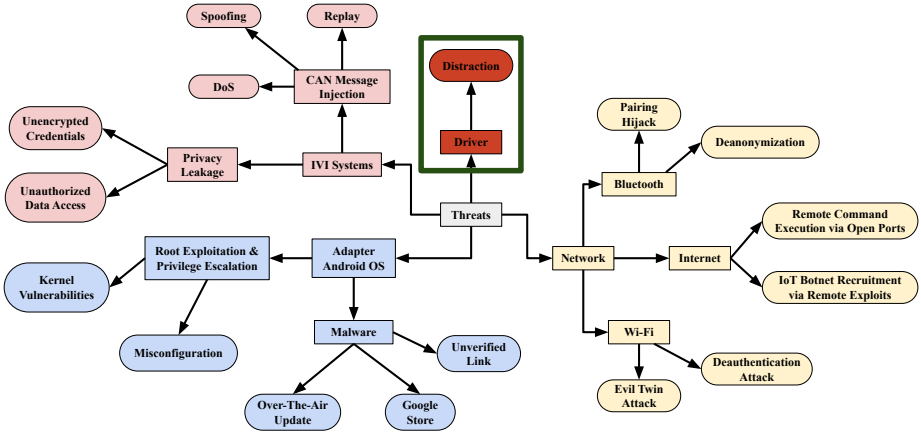
Why?



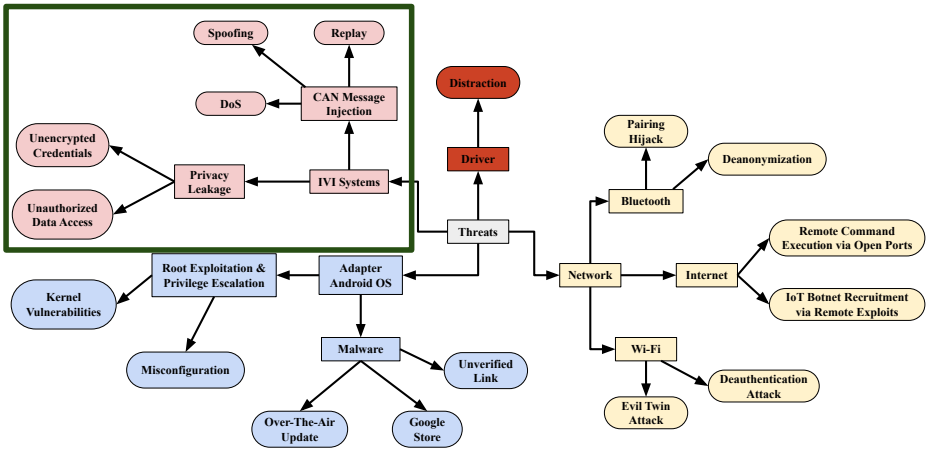
Security & Safety Assessment



Driver


Spoofing
Replay
DoS
CAN Message Injection
Distraction
Driver
Unencrypted Credentials
Privacy Leakage
IVI Systems
Unauthorized Data Access
Pairing Hijack
Deanonymization
Bluetooth
Threats
Remote Command Execution via Open Ports
Root Exploitation & Privilege Escalation
Adapter Android OS
Network
Internet
IoT Botnet Recruitment via Remote Exploits
Kernel Vulnerabilities
Malware
Wi-Fi
Misconfiguration
Unverified Link
Deauthentication Attack
Over-The-Air Update
Google Store
Evil Twin Attack

Infotainment



Infotainment



Infotainment





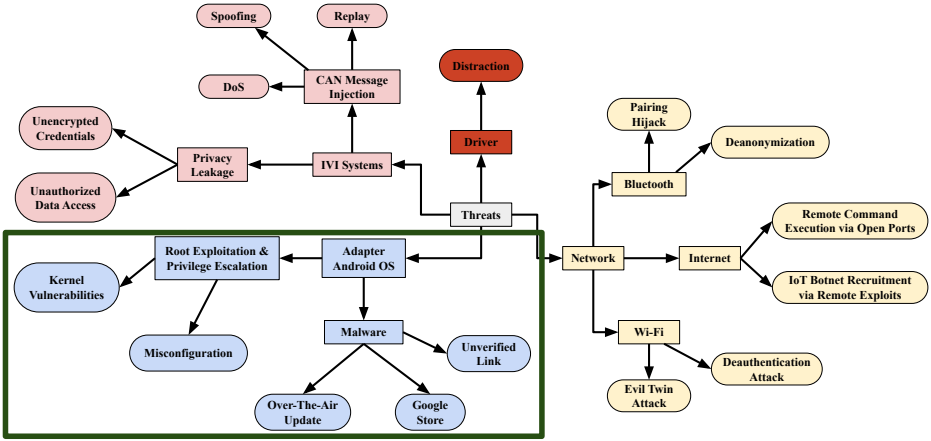
Infotainment







Android OS


Spoofing
Replay
DoS
CAN Message Injection
Distraction
Unencrypted Credentials
Privacy Leakage
IVI Systems
Driver
Unauthorized Data Access
Threats
Pairing Hijack
Deanonymization
Bluetooth
Remote Command Execution via Open Ports
Root Exploitation & Privilege Escalation
Adapter Android OS
Network
Internet
Kernel Vulnerabilities
IoT Botnet Recruitment via Remote Exploits
Malware
Wi-Fi
Misconfiguration
Unverified Link
Deauthentication Attack
Over-The-Air Update
Google Store
Evil Twin Attack

Android OS



Android OS





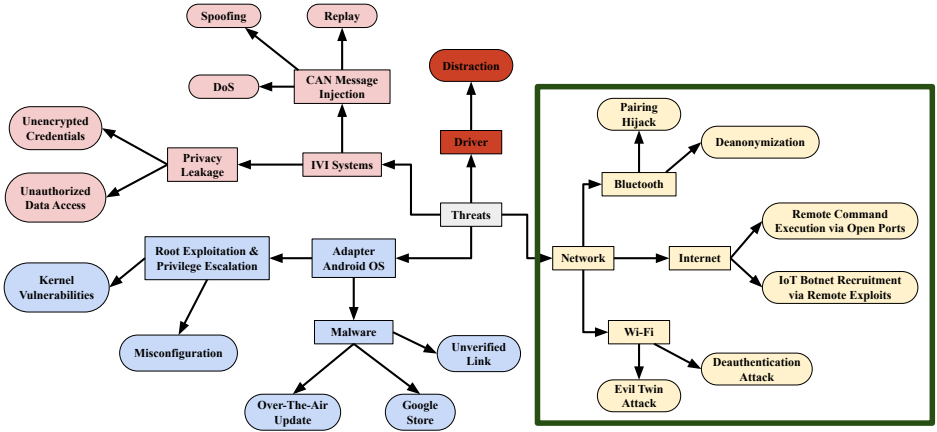
Android OS







Network


Spoofing
Replay
DoS
CAN Message Injection
Distraction
Unencrypted Credentials
Privacy Leakage
IVI Systems
Driver
Unauthorized Data Access
Threats
Root Exploitation & Privilege Escalation
Adapter Android OS
Kernel Vulnerabilities
Misconfiguration
Malware
Unverified Link
Over-The-Air Update
Google Store
Pairing Hijack
Deanonymization
Bluetooth
Remote Command Execution via Open Ports
Network
Internet
IoT Botnet Recruitment via Remote Exploits
Wi-Fi
Deauthentication Attack
Evil Twin Attack

Network

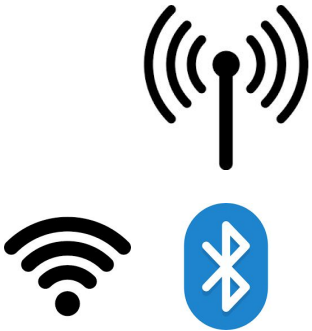


Network

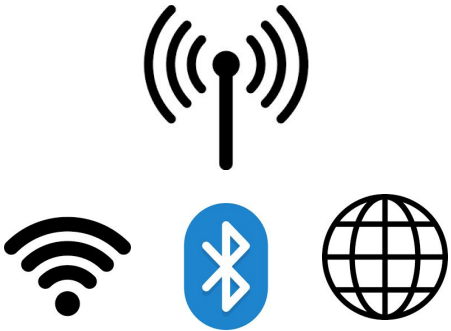




Network



Network

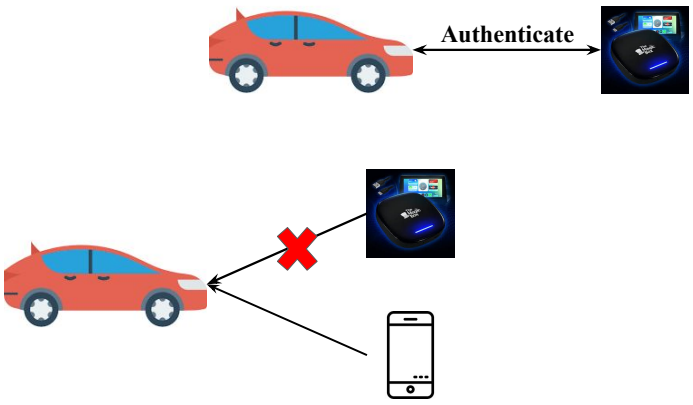


Mitigation

Mitigation

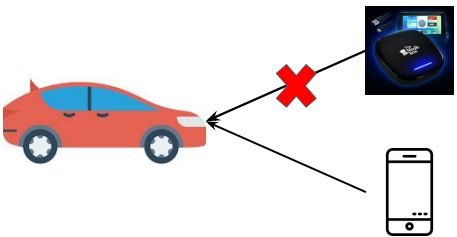


Mitigation



Mitigation







Q&A

SecLab @ OSU
https://go.osu.edu/seclab