German
OWASP
Day 2025

German OWASP Day 2025

Pwn My Ride

German OWASP Day 2025

oligo

Avi Lumelsky
AI Security Researcher
Oligo Security

German OWASP Day 2025

oligo

Uri Katz
Lead Researcher
Oligo Security

German OWASP Day 2025

Agenda

01 Intro to AirPlay, iAP2 and CarPlay

02 Vulnerability Discovery

03 Exploitation path to CarPlay

04 iAP2 deep dive

05 Implications: supply chain & trust in SDKs

06 Summary

German OWASP Day 2025

Agenda

01 Intro to AirPlay, iAP2 and CarPlay

02 Vulnerability Discovery

03 Exploitation path to CarPlay

04 iAP2 deep dive

05 Implications: supply chain & trust in SDKs

06 Summary

German OWASP Day 2025

AirBorne

23
Vulnerabilities

17
CVEs Assigned

0-CLICK RCE
Wormable Exploit

Billions
Affected Devices

DISCLOSURE TIMELINE

October 2024 — April 2025

German OWASP Day 2025

AirBorne

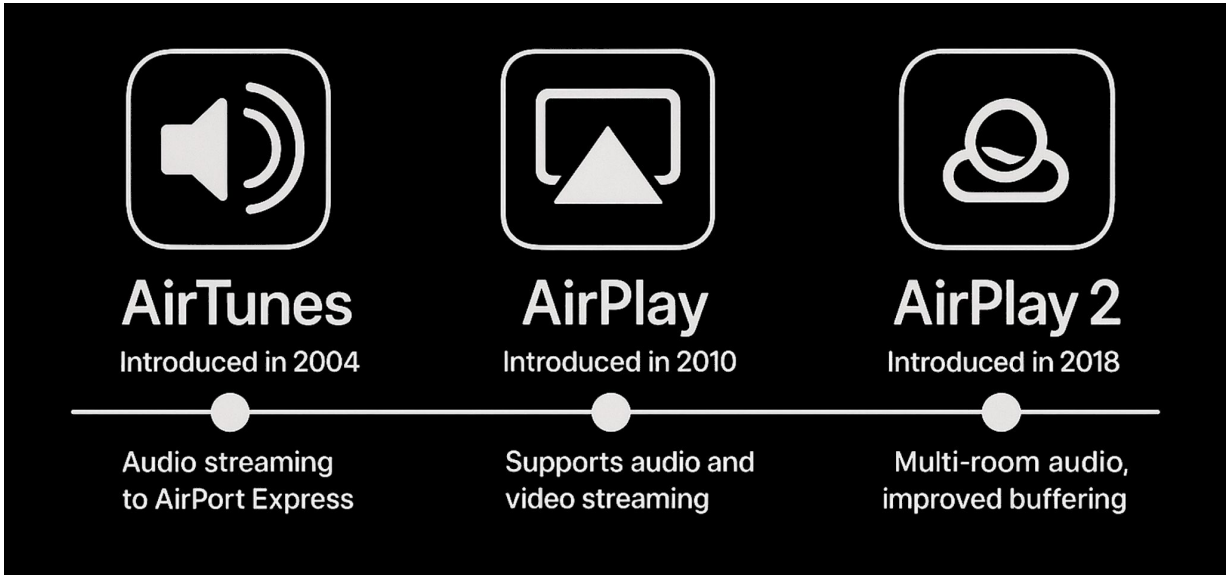
Works with Apple AirPlay

iAP2

CVE-2025-24132

German OWASP Day 2025

What is AirPlay?



German OWASP Day 2025

Vulnerability Discovery - AirPlay SDK

CarPlay

Overview Models

More than 800 models to choose from.

It's easier than ever to find a vehicle that works with CarPlay. Check this list for the latest information.*

Supports car keys

Stream video and audio with AirPlay

With AirPlay, you can stream video and audio from your iPhone, iPad, or another Mac to your Mac. This means that you can use your Mac as a display or speaker for your other devices. You can also stream from your Mac to an HDTV, or mirror what's on your Mac computer's screen.

Home app

Overview Accessories

AirPlay-Enabled TVs and Video Accessories

- AIWA Roku TV
- Amazon Fire TV 4-Series (2021)
- Amazon Fire TV Omni-Series (2021)
- Amazon Fire TV Smart TV (2K HD)
- Amazon Fire TV Smart TV (4K UHD)
- AOC Roku TV
- ATVIO Roku TV
- Coocaa Roku TV
- Daewoo Roku TV
- Element Roku TV
- FFalcon Roku TV
- FUNAI 4K Fire TV搭載スマートテレビ F340シリーズ (2022)
- FUNAI HD Fire TV搭載スマートテレビ F140シリーズ (2022)
- Hisense 4K UHD (2022)
- Hisense A63H Series (2022,2023)
- Hisense A65H Series (2022)
- Hisense A6H Series (2022)
- Hisense A6HAU Series (2022)
- Hisense A6K Series (2023)
- Hisense A7H Series (2022)
- Hisense A7K Series (2023)
- Hisense A85H Series (2022, 2023)
- Hisense A85K Series (2023)
- Hisense A9H Series (2022, 2023)
- Hisense C1 Series (2023)
- Hisense E7H (43″ 50″) Series (2022, 2023)
- Hisense E7K Series (2023)
- Hisense E7KQ PRO Series (2023)

German OWASP Day 2025

What is CarPlay?

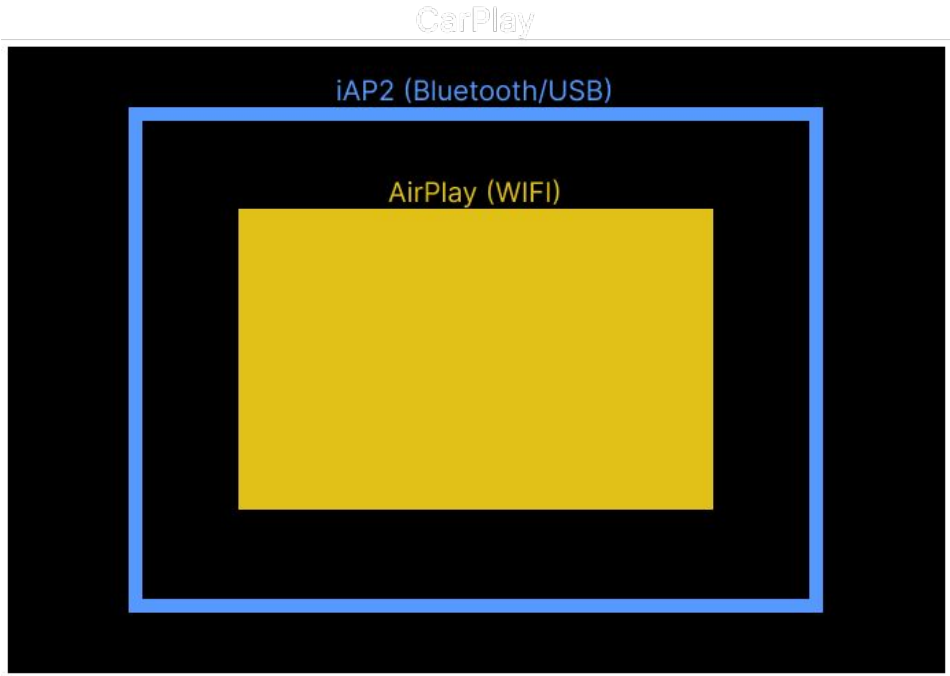
What is IAP2?

- iPod Accessory Protocol v2
- Connects Apple devices to accessories.
- Authentication, capabilities negotiation, launching apps (like CarPlay), etc.
- Transports: USB, Lightning, Bluetooth.

German OWASP Day 2025

AirPlay vs Wireless CarPlay

- iAP2 is used to negotiate the device WiFi Password
- Phone connects to the CarPlay device WiFi
- Phone initiates screen mirroring via AirPlay while connected to the device WiFi



German OWASP Day 2025

Agenda

01 Intro to AirPlay, iAP2 and CarPlay

02 Vulnerability Discovery

03 Exploitation path to CarPlay

04 iAP2 deep dive

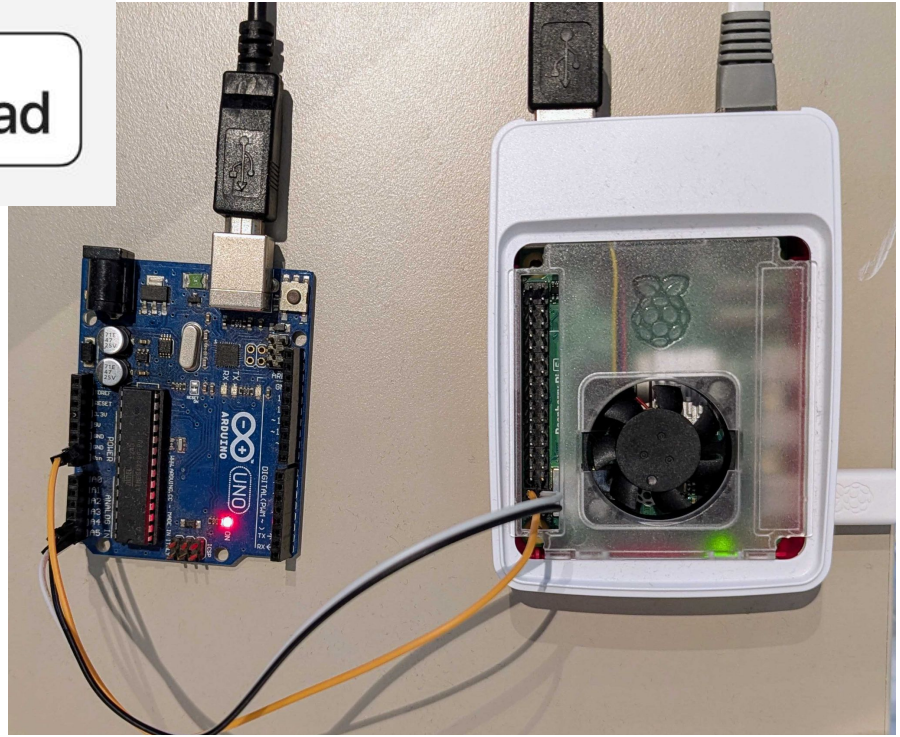
05 Implications: supply chain & trust in SDKs

06 Summary

German OWASP Day 2025

Simulating the SDK

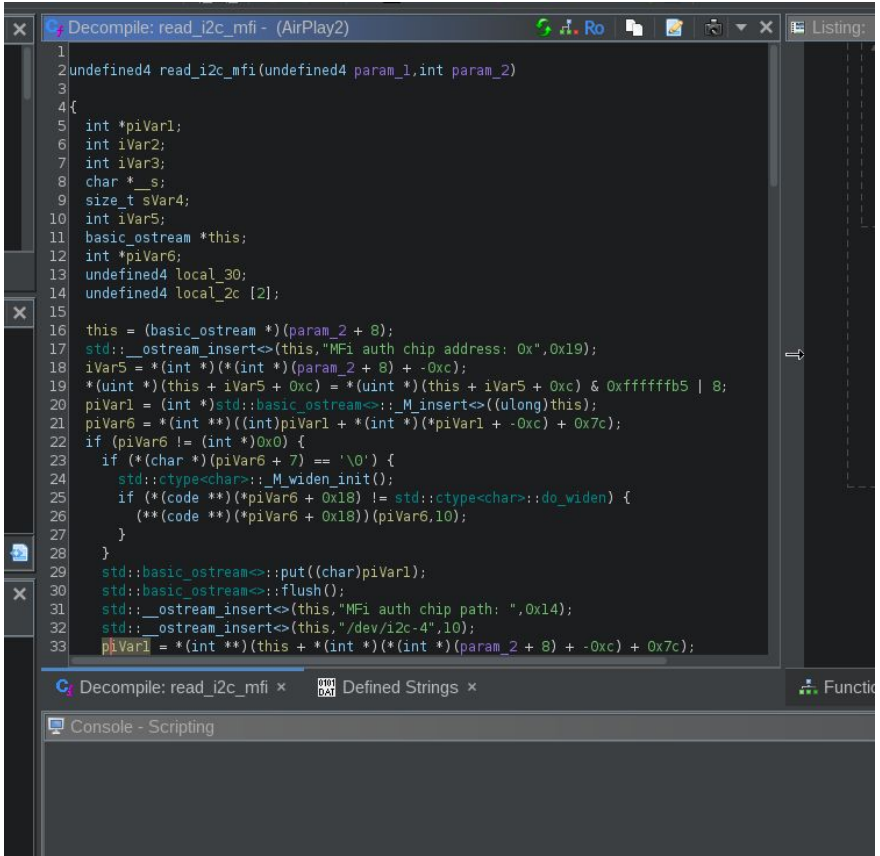
Made for iPhone | iPad



German OWASP Day 2025

Simulating the MFI chip

Firmware Binaries

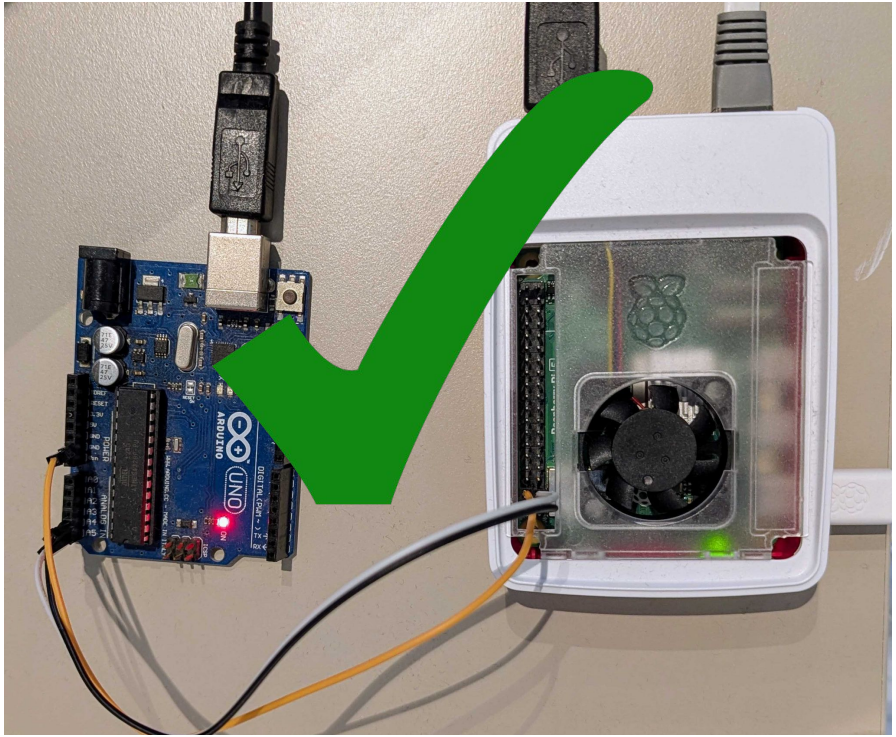


Arduino MFI simulation Code

```
#include <Wire.h>

// Replace with your device's I2C address
#define I2C_ADDRESS 0x10

void setup() {
  Wire.begin(I2C_ADDRESS); // Initialize I2C with the specifiec
  Wire.onReceive(receiveEvent); // Set receive event handler
  Wire.onRequest(requestEvent); // Set request event handler
  Serial.begin(9600); // Optional for debugging
}

void loop() {
  // Main loop does nothing; I2C events are interrupt-driven
}

// Event handler for receiving data from the master
void receiveEvent(int bytes) {
  while (Wire.available()) {
    char c = Wire.read(); // Read each byte sent by the master
    Serial.print("Received: ");
    Serial.println(c); // Debug: Print received data
  }
}

// Event handler for responding to master requests
void requestEvent() {
  Wire.write(registerData); // Respond with the data in regist
    Serial.print("Register 0x31 read, sending: ");
    Serial.println(registerData, HEX);
}
```

German OWASP Day 2025

Simulating the SDK



Vulnerability discovery - Final POC

- Running AirPlay Server ✅
- But, is the product vulnerable?

German OWASP Day 2025

Exploiting Over WiFi – Stack Overflow RCE

```
bash-4.3# id
id
uid=0(root) gid=0(root)
```

German OWASP Day 2025

Are you Patched?

CVE-2025-24132 Detail

Description

The issue was addressed with improved memory handling. This issue is fixed in AirPlay audio SDK 2.7.1, AirPlay video SDK 3.6.0.126, CarPlay Communication Plug-in R18.1. An attacker on the local network may cause an unexpected app termination.

German OWASP Day 2025

Are you Patched?

CVE-2025-24132 Detail

Description

The issue was addressed with improved memory handling. This issue is fixed in AirPlay audio SDK 2.7.1, AirPlay video SDK 3.6.0.126, CarPlay Communication Plug-in R18.1. An attacker on the local network may cause an unexpected ~~app termination~~.

unexpected Remote Code Execution

German OWASP Day 2025

Agenda

01 Intro to AirPlay, iAP2 and CarPlay

02 Vulnerability Discovery

03 Exploitation path to CarPlay

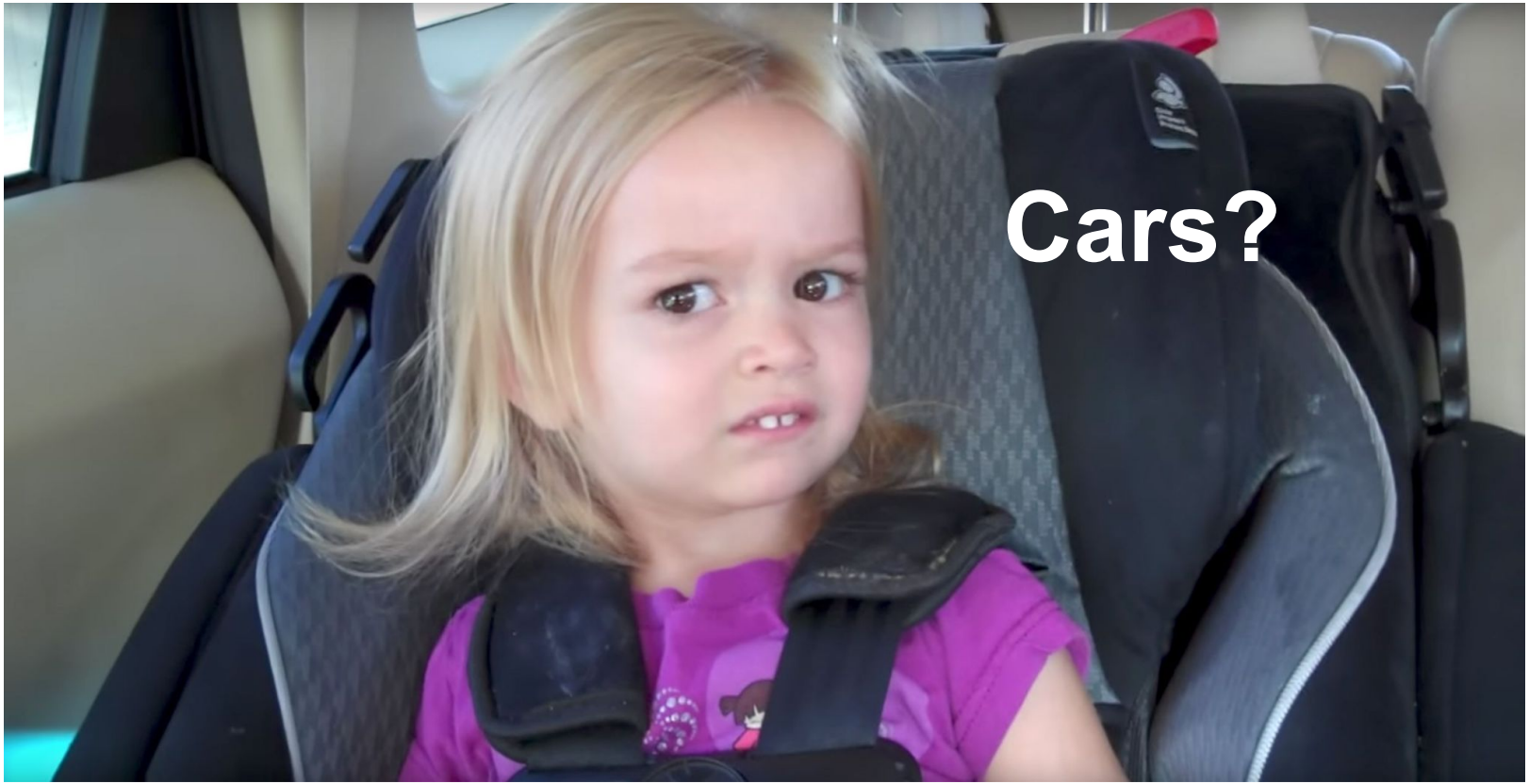
04 iAP2 deep dive

05 Implications: supply chain & trust in SDKs

06 Summary

German OWASP Day 2022

Moving to Cars



German OWASP Day 2025

Moving to Cars

When you have limited budget

German OWASP Day 2025

How do we connect to the device WiFi?


Cars!
Pioneer
P2410-02996

German OWASP Day 2025

Agenda

01 Intro to AirPlay, iAP2 and CarPlay

02 Vulnerability Discovery

03 Exploitation path to CarPlay

04 iAP2 deep dive

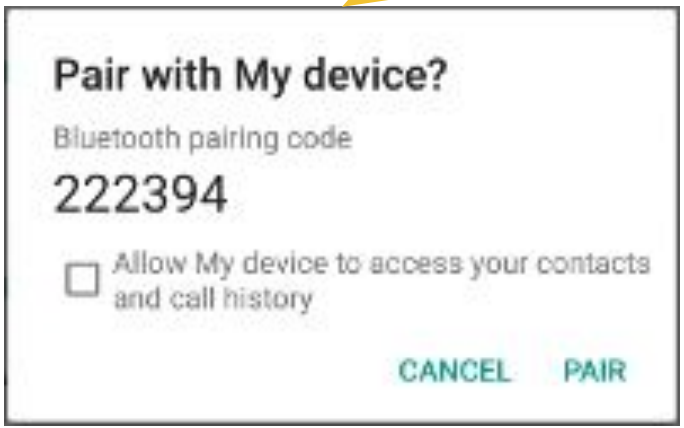
05 Implications: supply chain & trust in SDKs

06 Summary

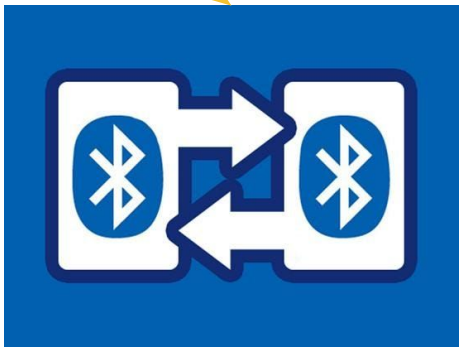
German OWASP Day 2025

Bluetooth pairing

PIN/ Passkey



No-Pin (Just Works)



German OWASP Day 2025

iAP2 Protocol Structure

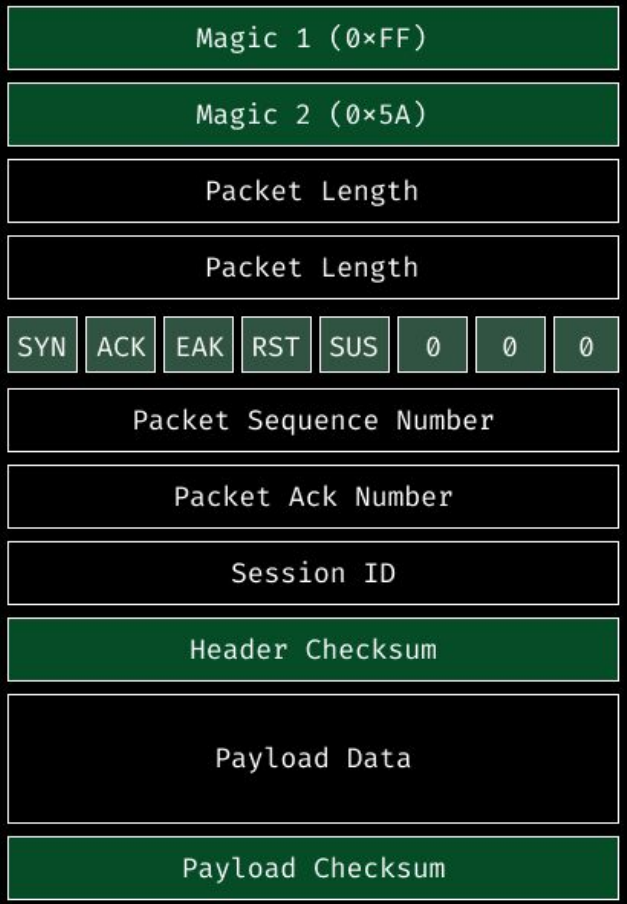
iAP2

Wi Fi

Apple CarPlay

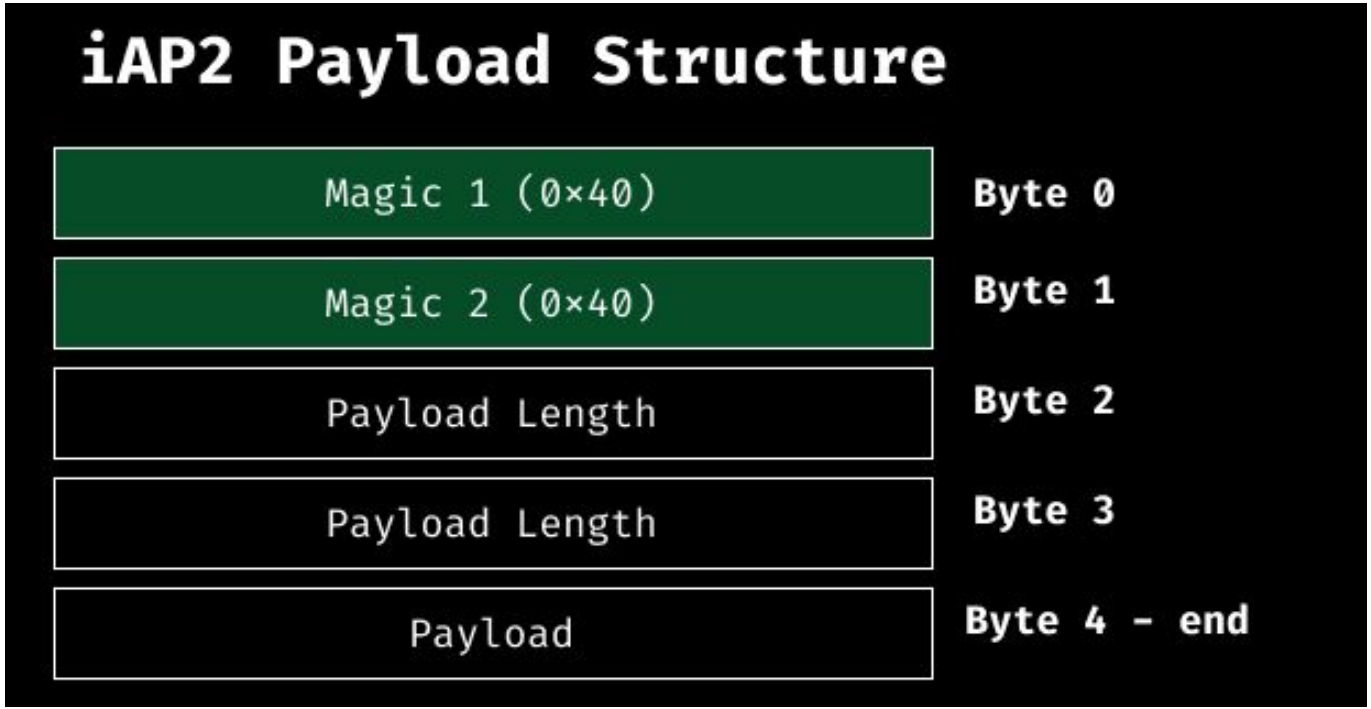
German OWASP Day 2025

iAP2 Packet Structure



German OWASP Day 2025

iAP2 Payload Structure



German OWASP Day 2025

iAP2 Checksum

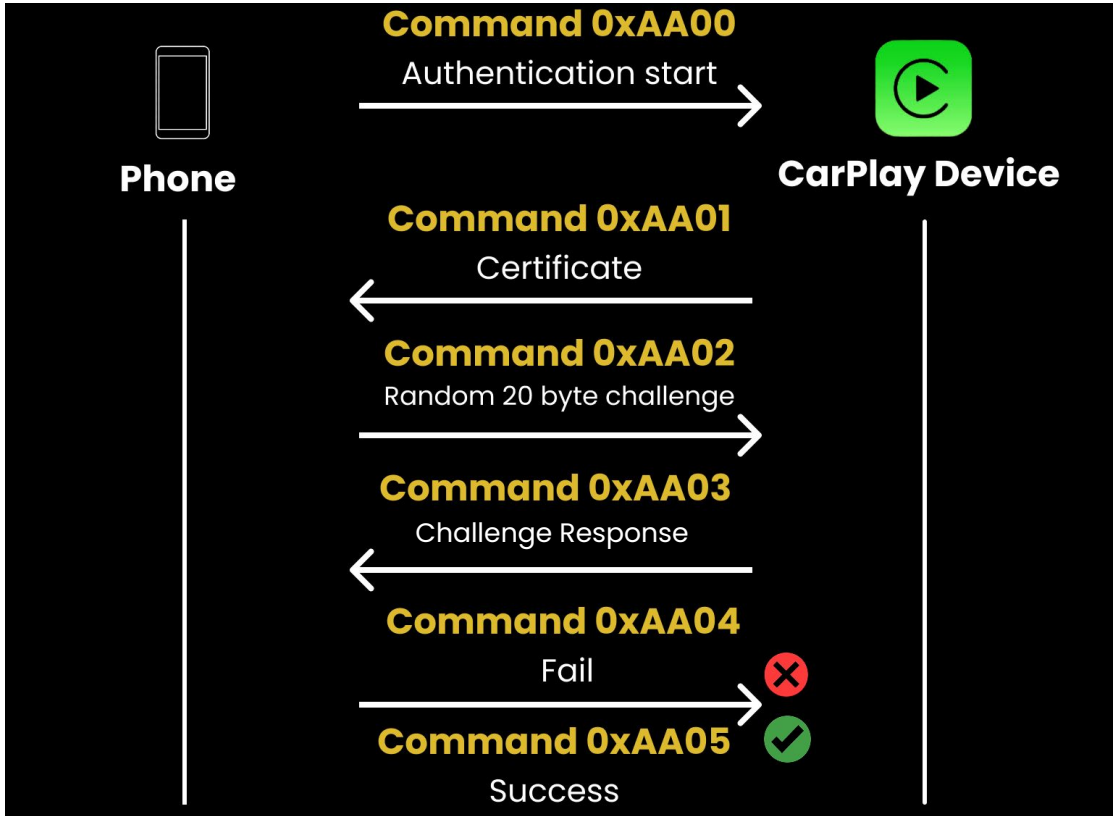
```
def iap2_calc_checksum(buffer: bytes) -> bytes:  2 usages
    if buffer and len(buffer) > 0:
        checksum = sum(buffer) & 0xFF
        checksum = (0x100 - checksum) & 0xFF
        checksum = struct.pack( fmt: "B",  *v: checksum)
        return checksum
    else:
        print("Error: NULL buffer or length is 0!")
    return b""
```

iAP2 Authentication

- Authentication is **one way**
- The phone authenticates the device
- The device **does not** authenticate the phone
- **Any device can impersonate a phone**

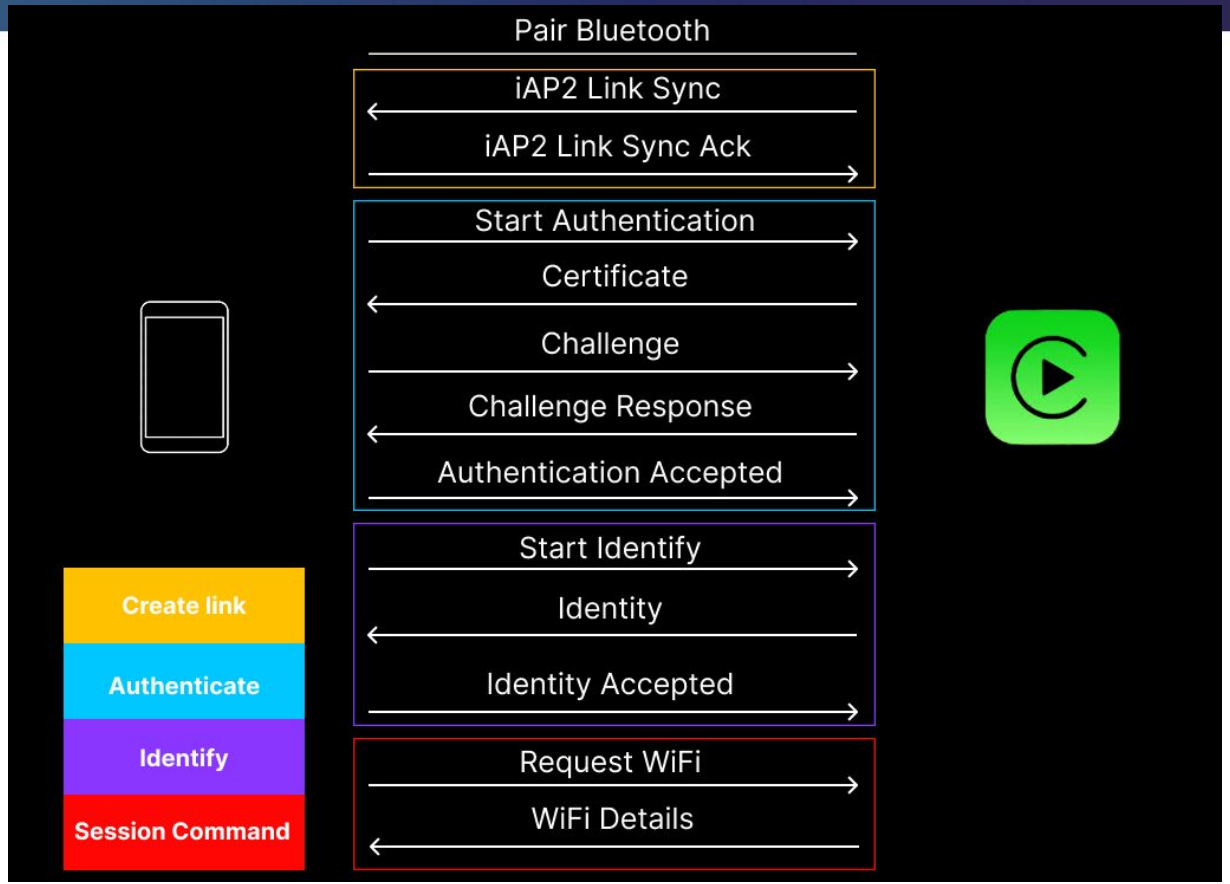
German OWASP Day 2025

Authentication steps



German OWASP Day 2025

iAP2 Session

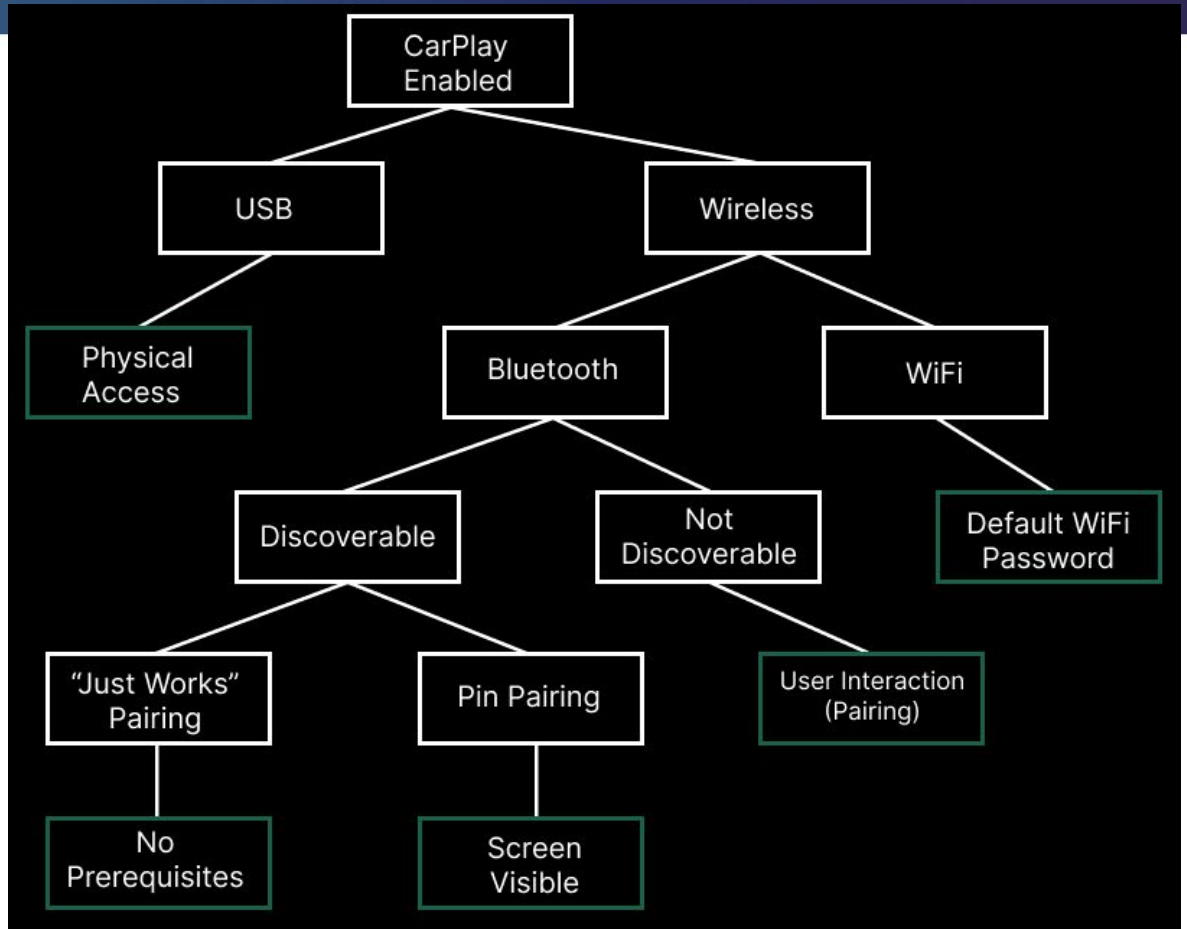


German OWASP Day 2025

iAP2 Wifi Credentials

German OWASP Day 2025

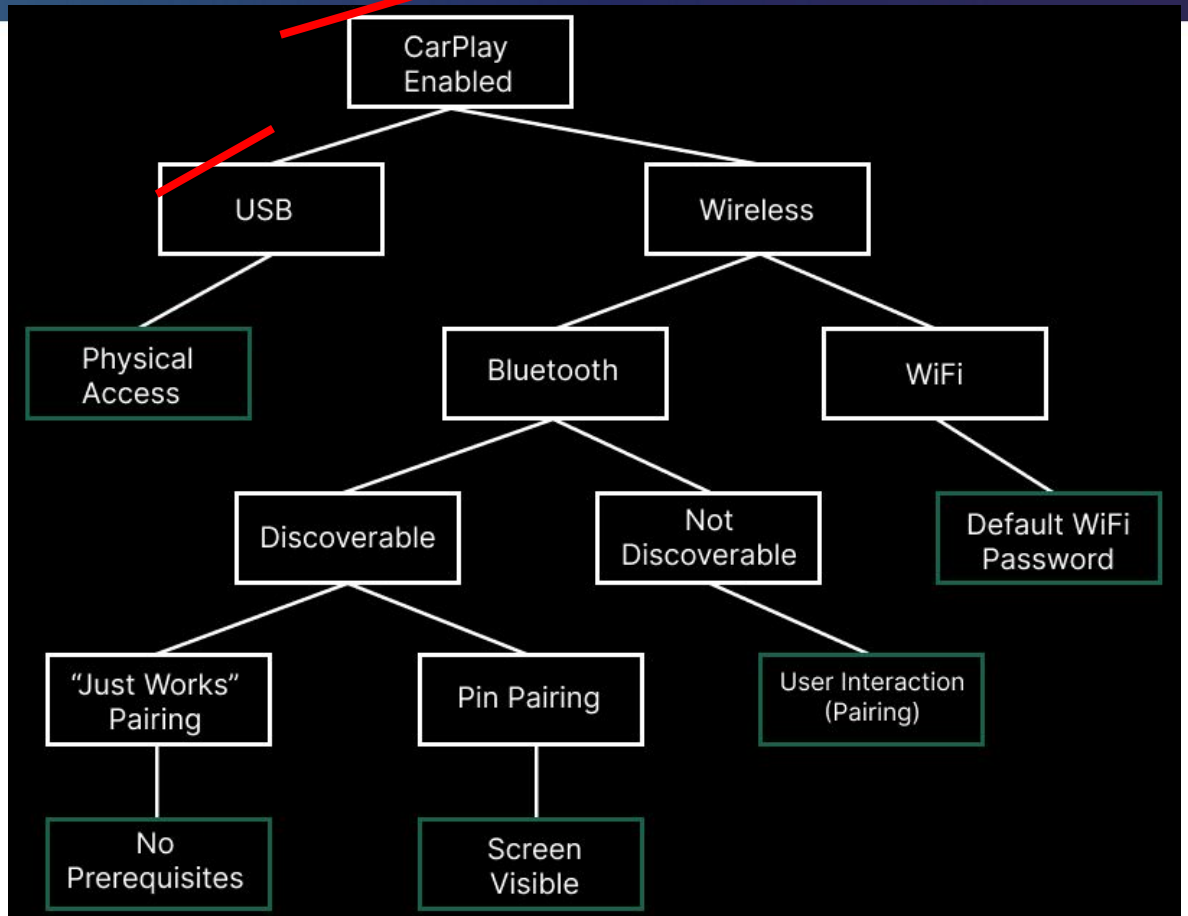
Prerequisites



German OWASP Day 2025

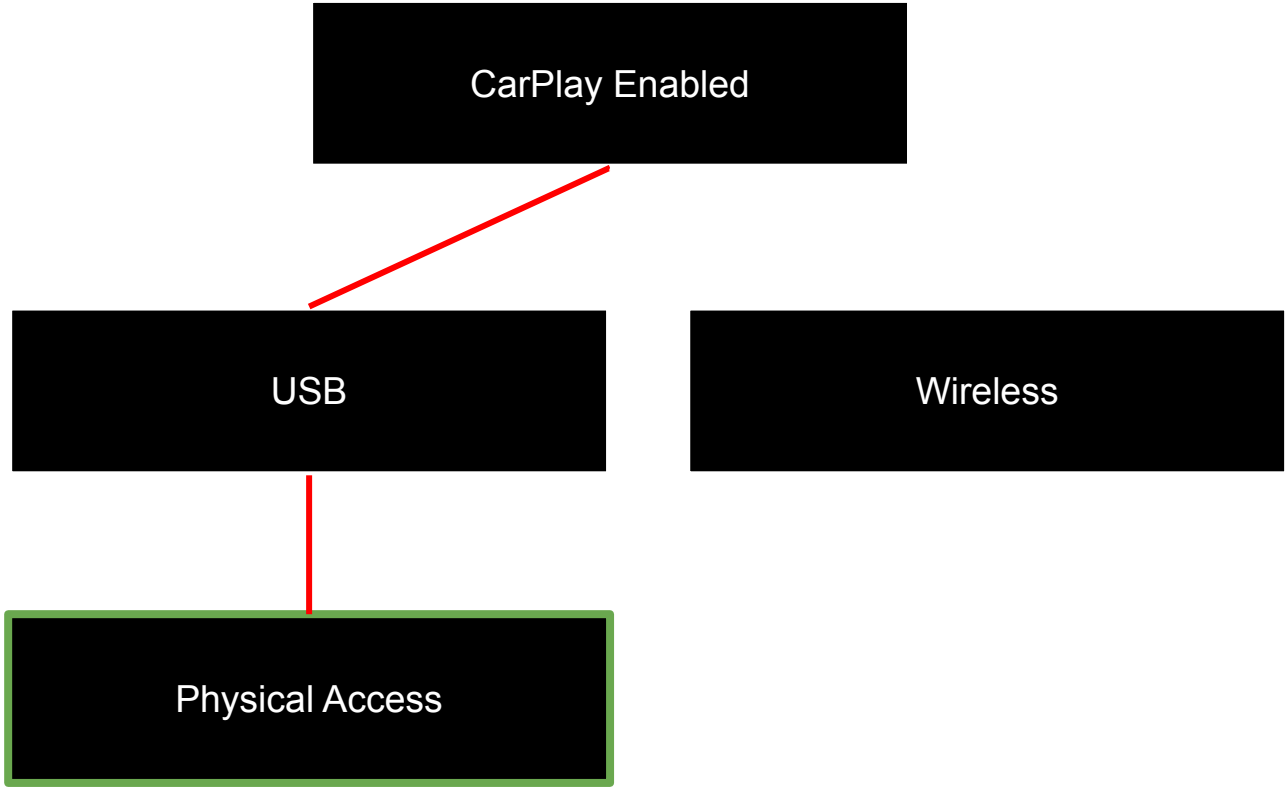
Prerequisites

1/5



German OWASP Day 2025

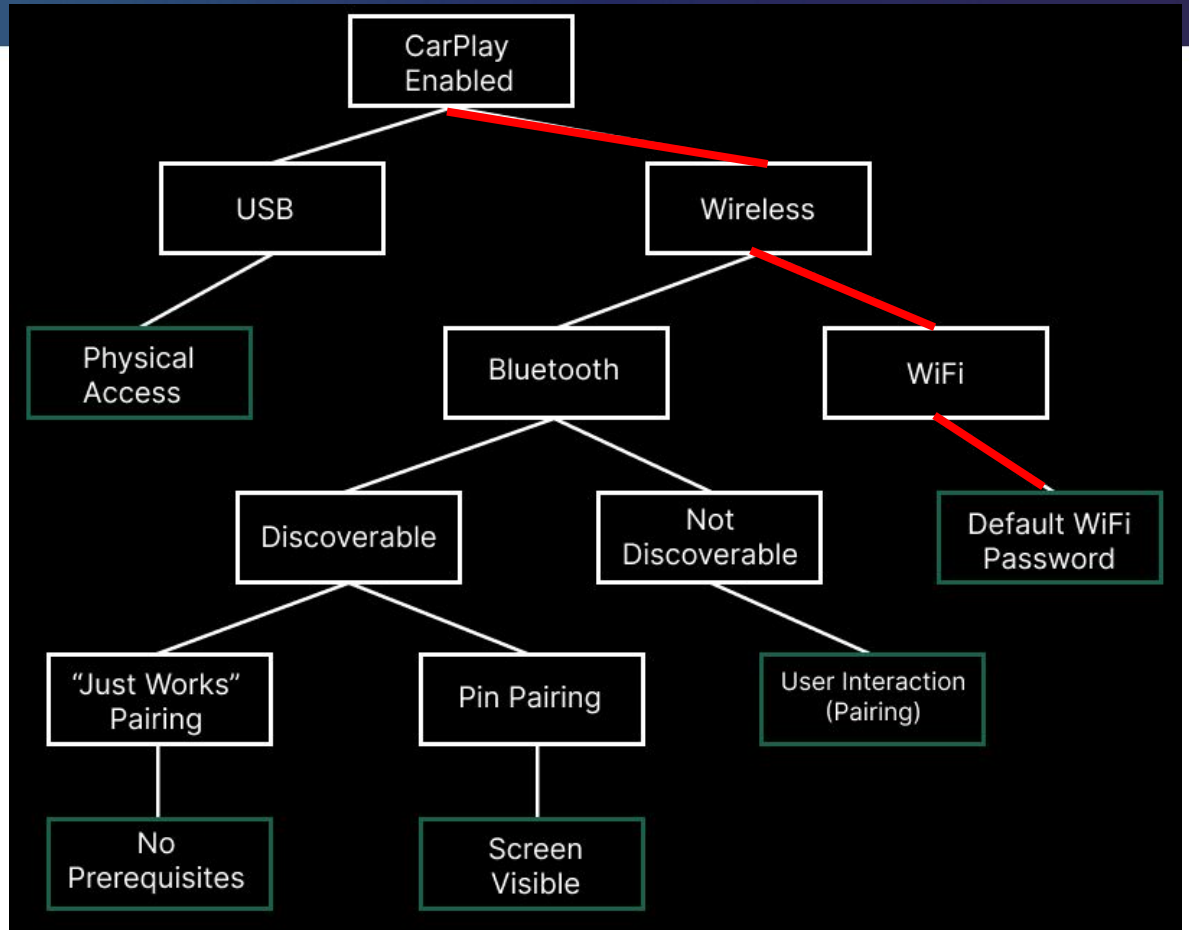
Prerequisites



German OWASP Day 2025

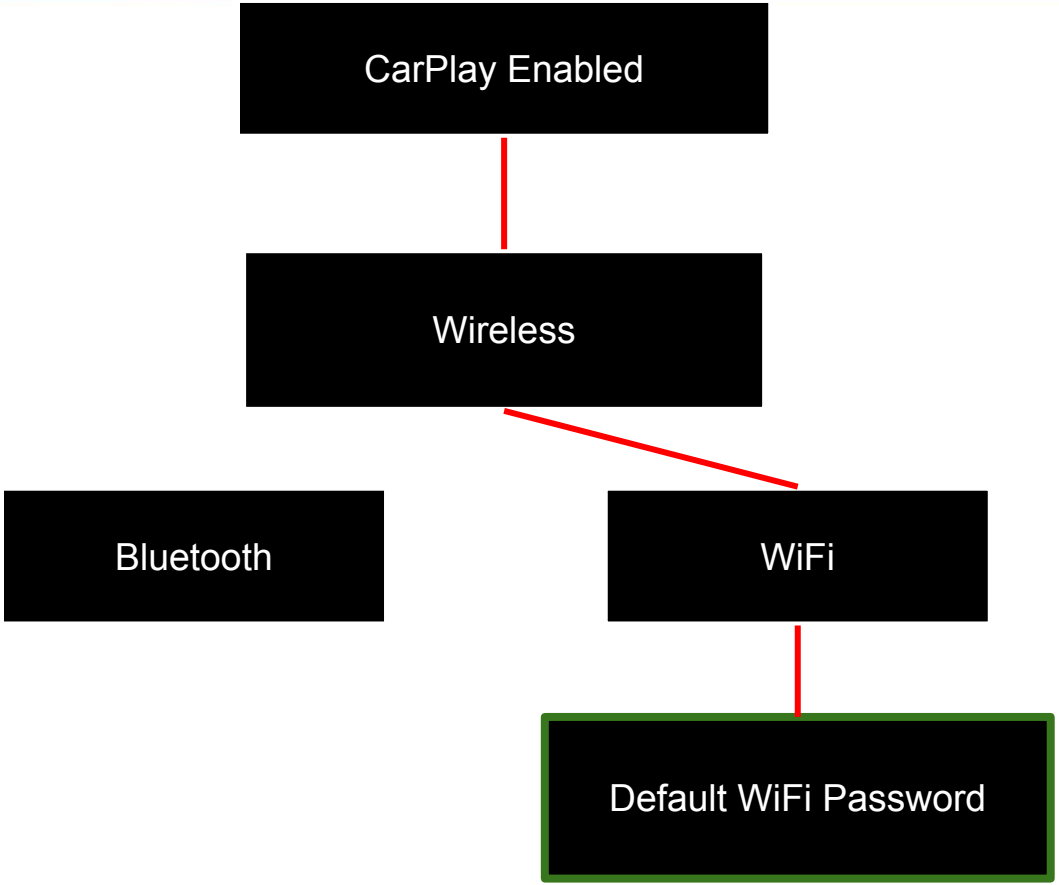
Prerequisites

2/5



German OWASP Day 2025

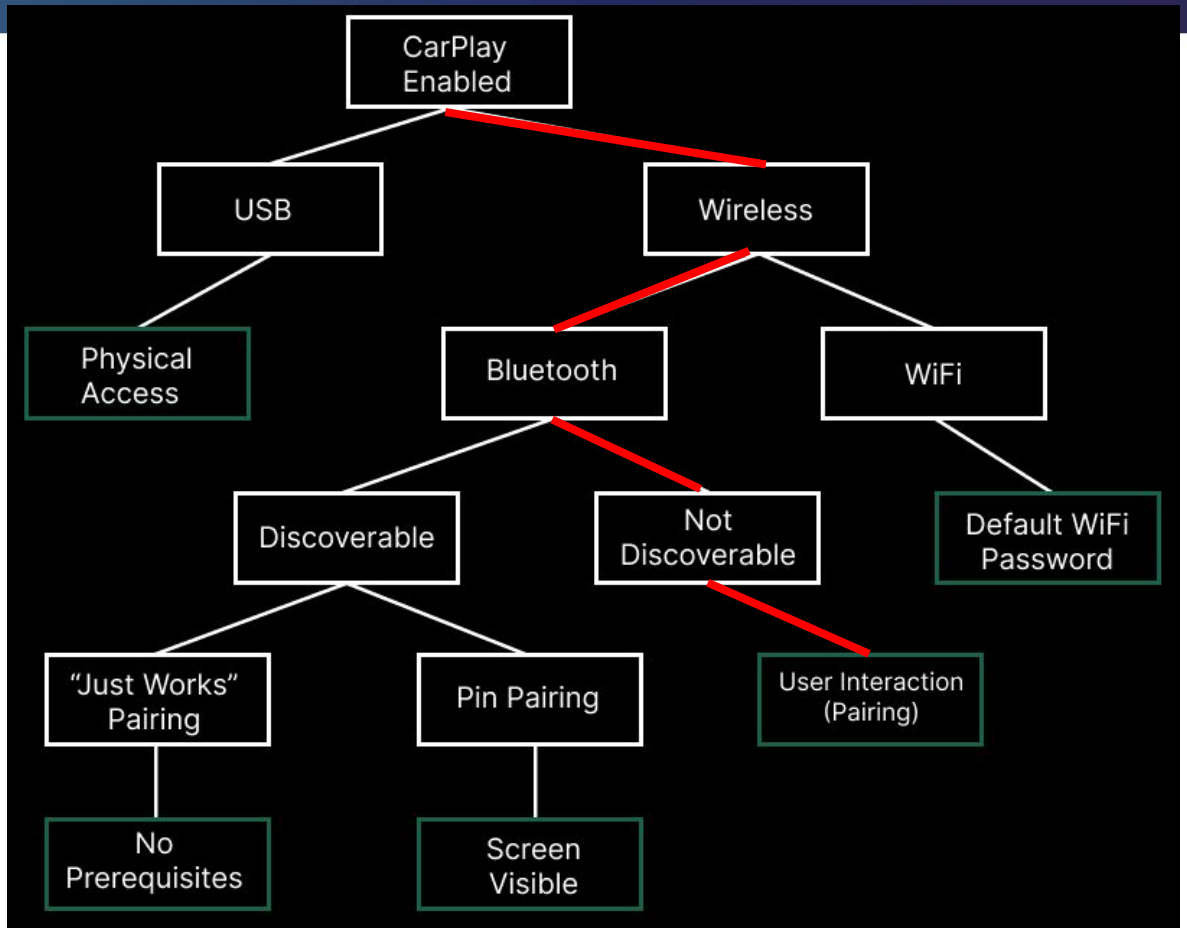
Prerequisites



German OWASP Day 2025

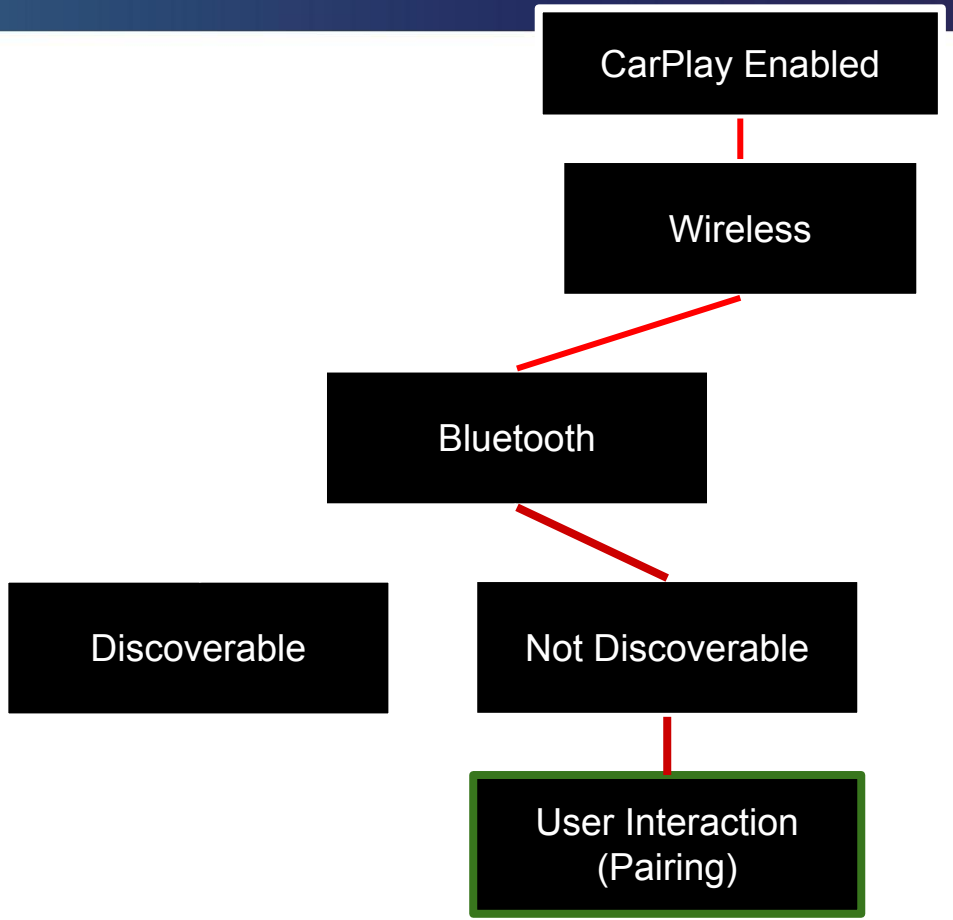
Prerequisites

3/5



German OWASP Day 2025

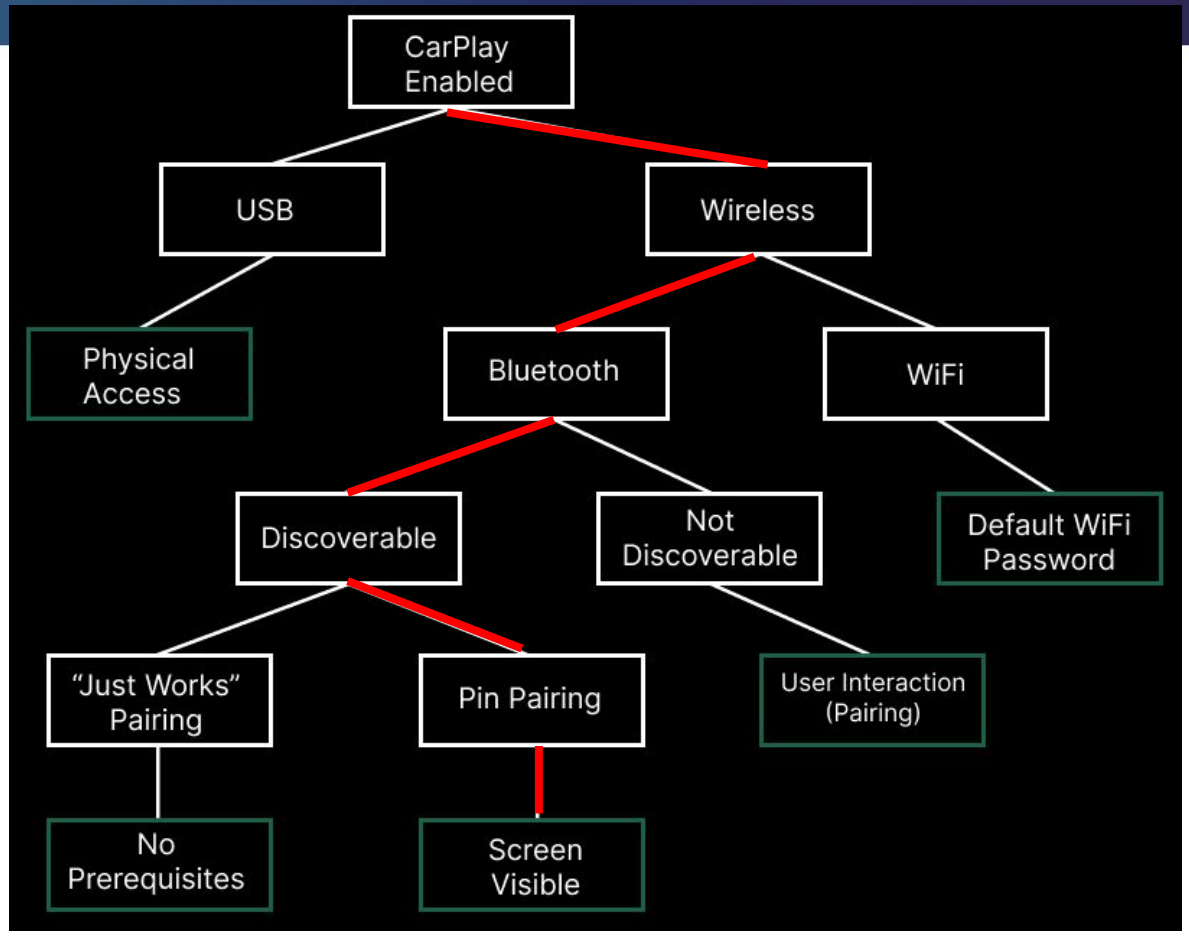
Prerequisites



German OWASP Day 2025

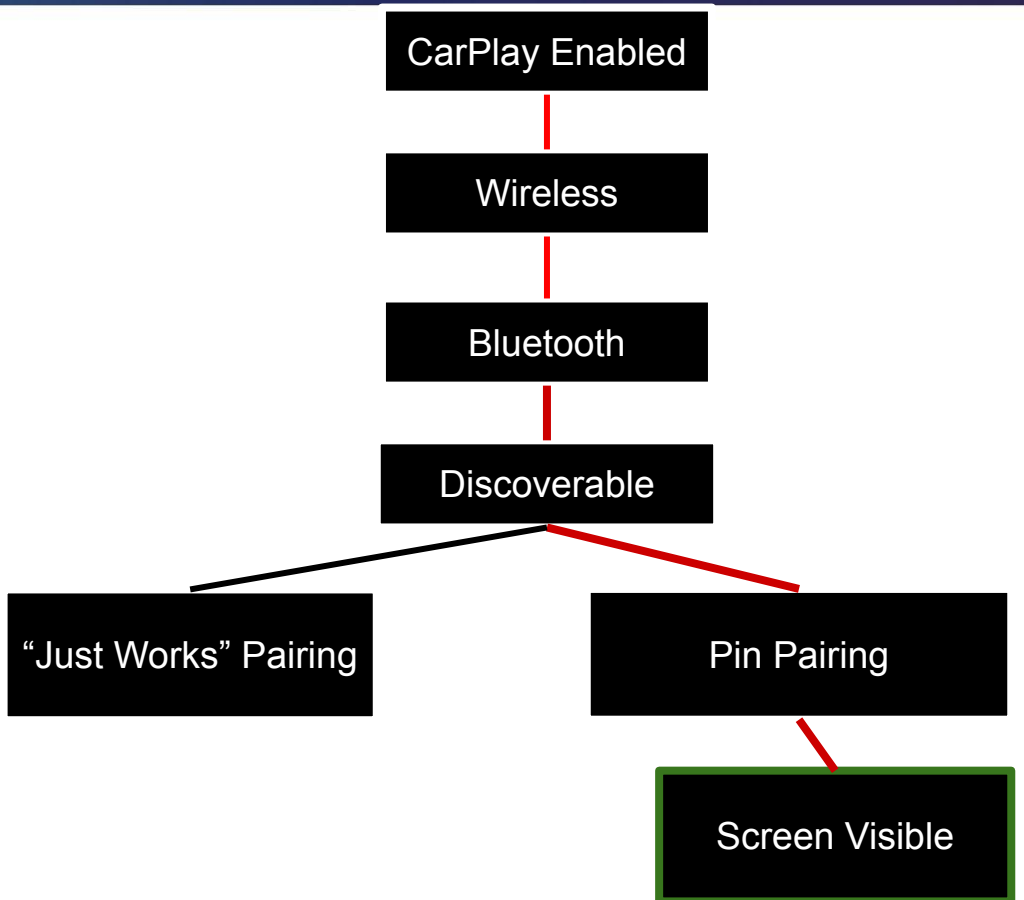
Prerequisites

4/5



German OWASP Day 2025

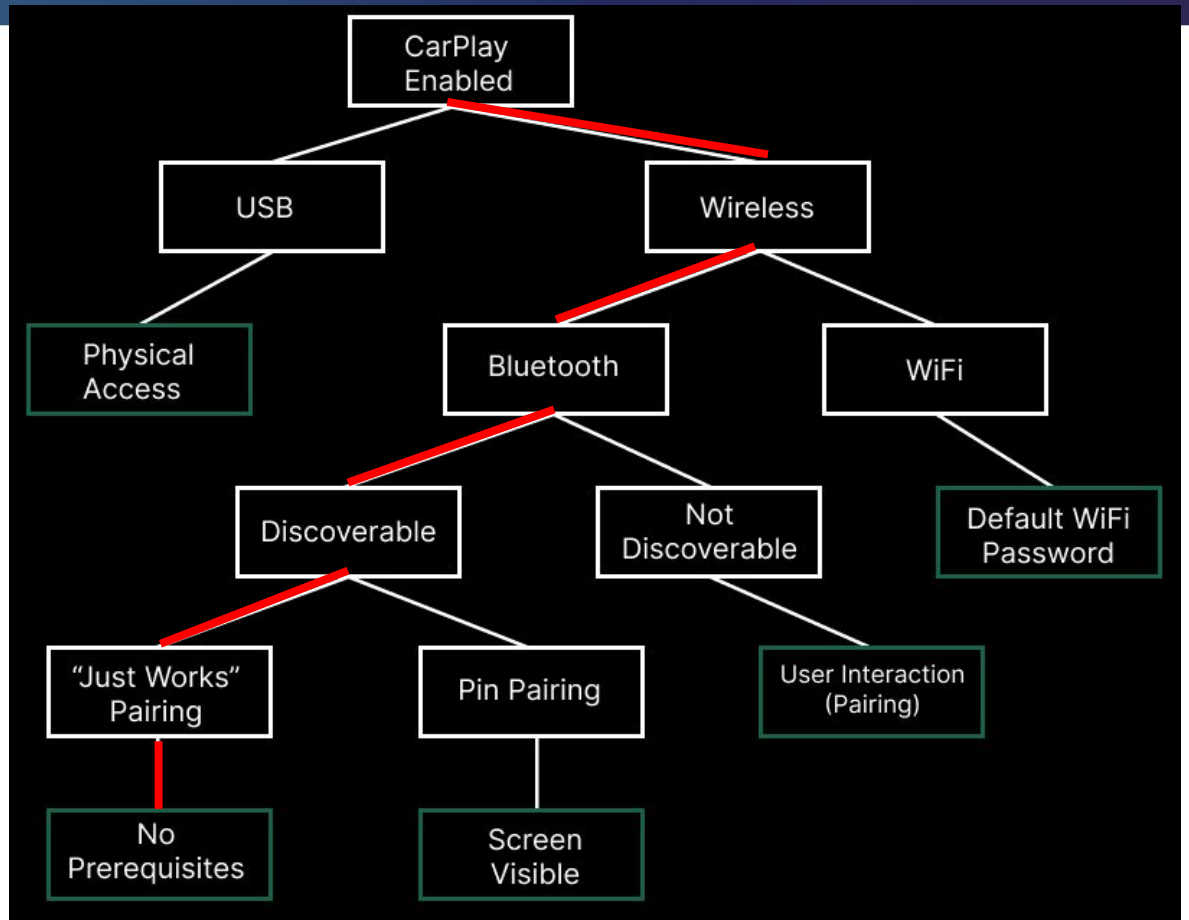
Prerequisites



German OWASP Day 2025

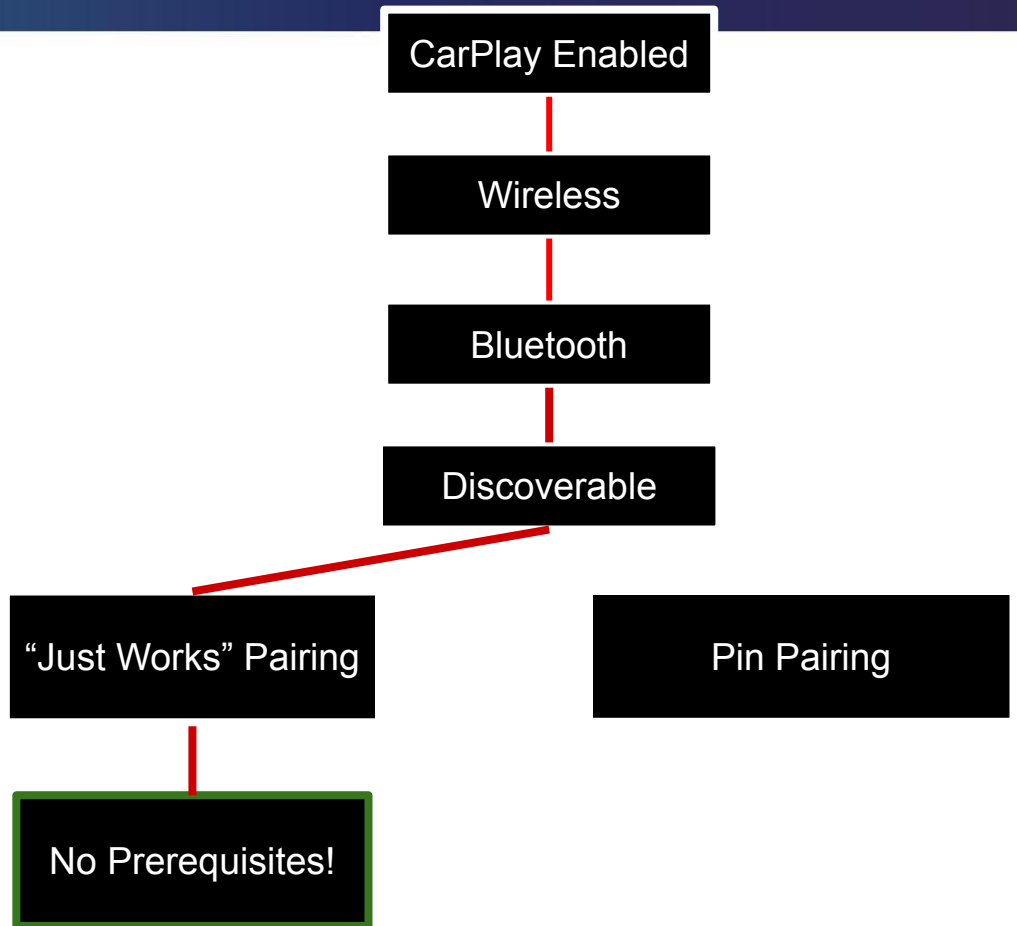
Prerequisites

5/5



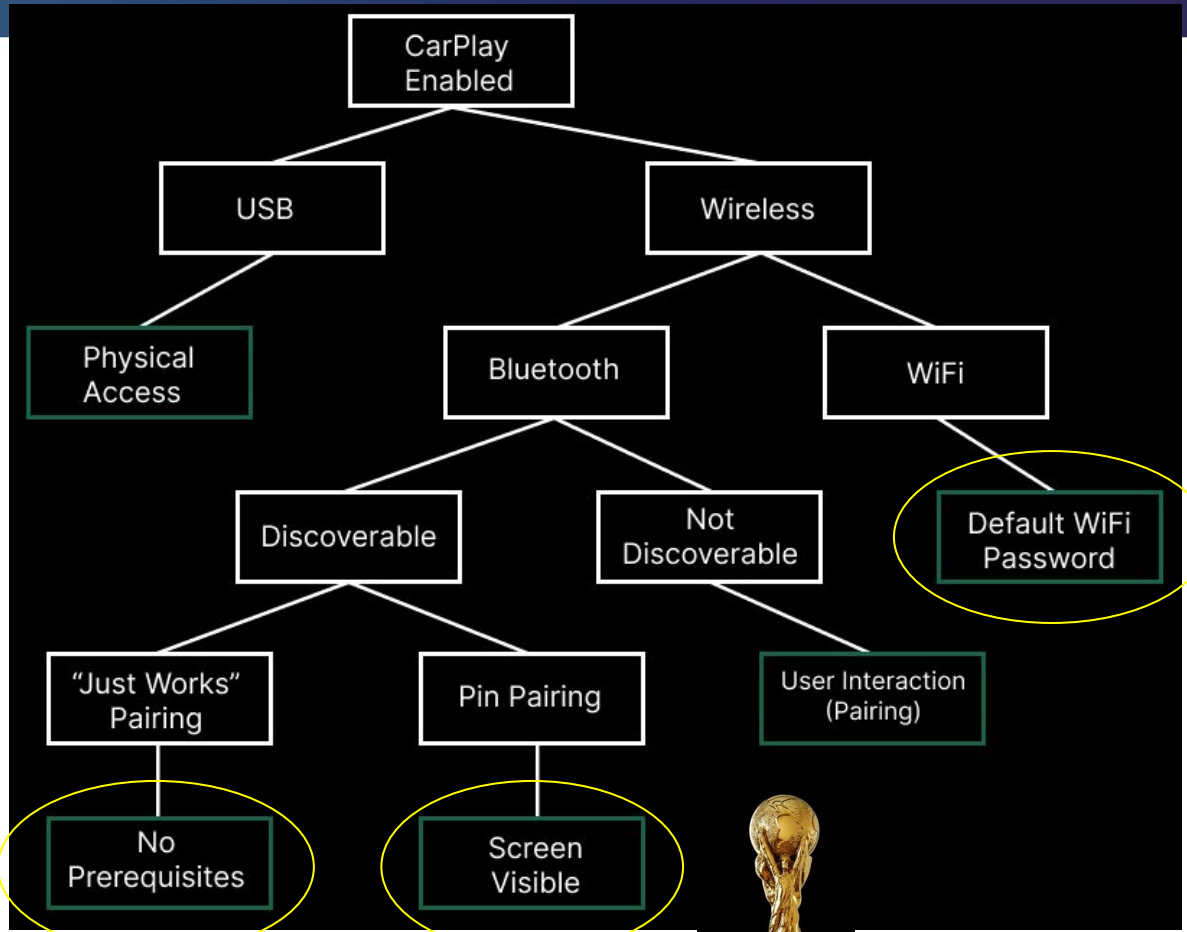
German OWASP Day 2025

Prerequisites



German OWASP Day 2025

Prerequisites



DEMO


AIRBORNE
CVE-2025-24132

German OWASP Day 2025

Agenda

01 Intro to AirPlay, iAP2 and CarPlay

02 Vulnerability Discovery

03 Exploitation path to CarPlay

04 iAP2 deep dive

05 Implications: supply chain & trust in SDKs

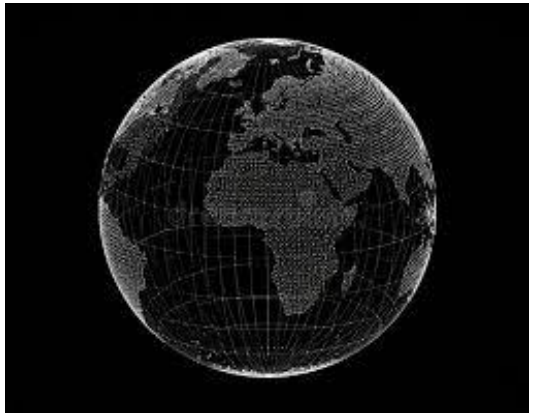
06 Summary

German OWASP Day 2025

The Problem: The SDK Supply Chain

“Not my code” ≠ “Not my problem”

Implications



Millions of vehicles & AirPlay SDK Devices impacted

Firmware updates for cars could take **years**

Drive-by Bluetooth Attacks

German OWASP Day 2025

Agenda

01 Intro to AirPlay, iAP2 and CarPlay

02 Vulnerability Discovery

03 Exploitation path to CarPlay

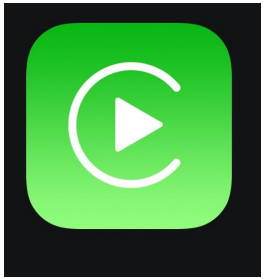
04 iAP2 deep dive

05 Implications: supply chain & trust in SDKs

06 Summary

German OWASP Day 2025

Summary



German OWASP Day 2025

Questions?

Pwn My Ride

German OWASP Day 2025

Thank You!

oligo

Avi Lumelsky

avi@oligosecurity.io

@avi_lum

German OWASP Day 2025

THANK YOU!

oligo

German
OWASP
Day 2025

German OWASP Day 2025

PRESENTATION TITLE ON EVERYTHING ABOUT APPLICATION SECURITY

JONATHAN DAVIS III

German OWASP Day 2025

01 TITLE OF THE FIRST GROUP OF SLIDES

SUB-HEADLINE

German OWASP Day 2025

THANK YOU!