



German
OWASP
Day 2025



German
OWASP
Day 2025

Pwn
My
Ride



Avi Lumelsky
AI Security Researcher
Oligo Security



German
OWASP
Day 2025



Uri Katz
Lead Researcher
Oligo Security



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**



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**



AirBorne



23

Vulnerabilities



17

CVEs Assigned



**0-CLICK
RCE**

Wormable Exploit



Billions

Affected Devices

DISCLOSURE TIMELINE

October 2024

April 2025

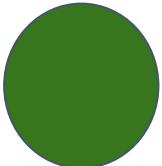


German
OWASP
Day 2025

AirBorne



!**CVE-2025-24132**



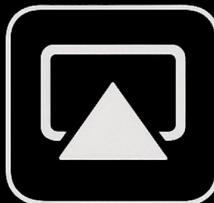


What is AirPlay?



AirTunes

Introduced in 2004



AirPlay

Introduced in 2010



AirPlay 2

Introduced in 2018

Audio streaming
to AirPort Express

Supports audio and
video streaming

Multi-room audio,
improved buffering



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

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)

Overview Accessories



What is CarPlay?





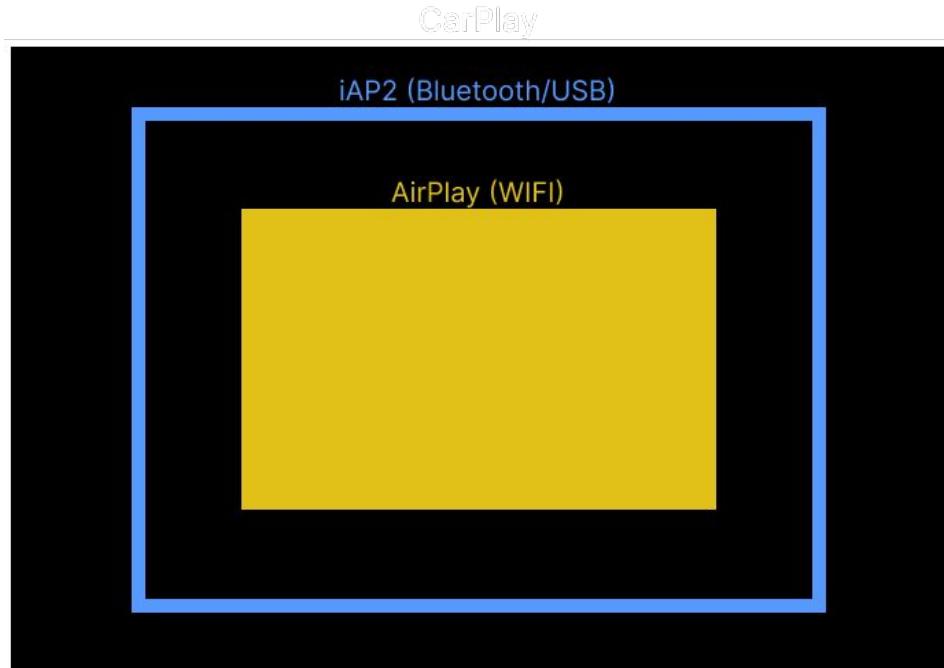
What is IAP2?

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



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



Agenda

01 **Intro to AirPlay, iAP2 and CarPlay**

04 **iAP2 deep dive**

02 **Vulnerability Discovery**

05 **Implications: supply chain & trust
in SDKs**

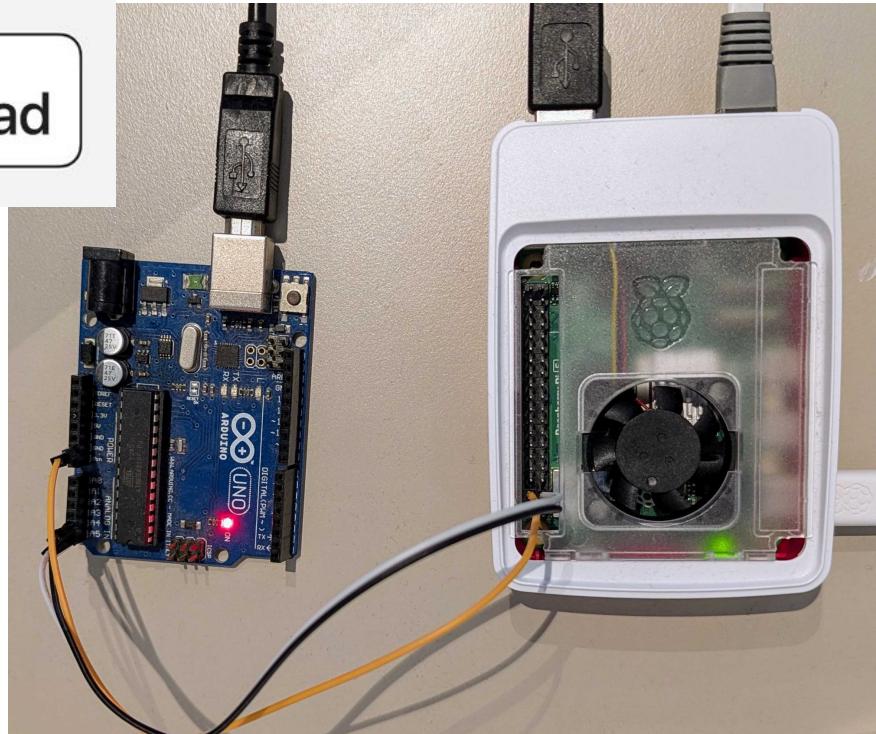
03 **Exploitation path to CarPlay**

06 **Summary**



Simulating the SDK

Made for
 iPhone | iPad





Simulating the MFI chip

Firmware Binaries

The screenshot shows a decompiler interface with the title "Decompile: read_i2c_mfi - (AirPlay2)". The code is written in assembly-like pseudocode:

```
1 undefined4 read_i2c_mfi(undefined4 param_1,int param_2)
2
3 {
4     int *iVar1;
5     int iVar2;
6     int iVar3;
7     char *_s;
8     size_t sVar4;
9     int iVar5;
10    basic_ostream *this;
11    int *iVar6;
12    undefined4 local_30;
13    undefined4 local_2c [2];
14
15    this = (basic_ostream *)param_2 + 8;
16    std::ostream insert<>(this,"MFI auth chip address: 0x",0x19);
17    iVar5 = *(int *)*(int *)param_2 + 8 + -0xc;
18    *(uint *)this + iVar5 + 0xc = *(uint *)this + iVar5 + 0xc & 0xfffffffffb5 | 8;
19    iVar1 = (int *)std::basic_ostream<>::_M_insert<>((ulong)this);
20    iVar6 = *(int **)((int) iVar1 + *(int *)(*iVar1 + -0xc) + 0x7c);
21    if (*iVar6 != (int *)0x0) {
22        if (*(*char *)(*iVar6 + 7) == '\0') {
23            std::ctype<char>::_M_widen_init();
24            if (*(*code **)(*iVar6 + 0x18) != std::ctype<char>::do_widen) {
25                (**code **)(*iVar6 + 0x18)(iVar6,10);
26            }
27        }
28        std::basic_ostream<>::put((char)iVar1);
29        std::basic_ostream<>::flush();
30        std::ostream_insert<>(this,"MFI auth chip path: ",0x14);
31        std::ostream_insert<>(this,"/dev/i2c-4",10);
32        iVar1 = *(int **)(this + *(int *)(*int *)param_2 + 8 + -0xc) + 0x7c;
33    }
```

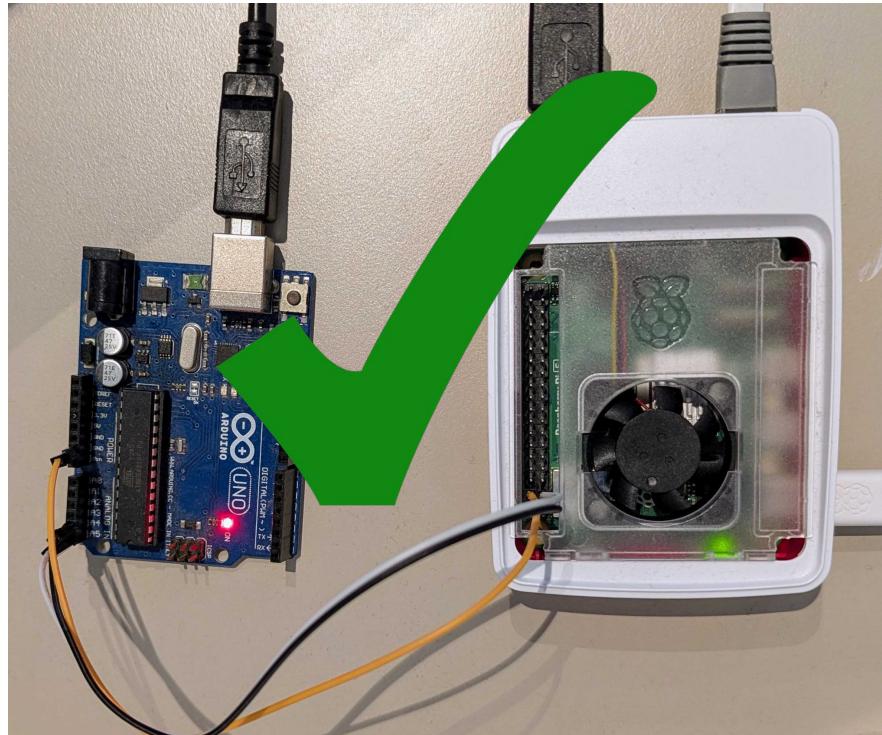
Console - Scripting

Arduino MFI simulation Code

```
1 #include <Wire.h>
2
3 // Replace with your device's I2C address
4 #define I2C_ADDRESS 0x10
5
6 void setup() {
7     Wire.begin(I2C_ADDRESS); // Initialize I2C with the specified
8     Wire.onReceive(receiveEvent); // Set receive event handler
9     Wire.onRequest(requestEvent); // Set request event handler
10    Serial.begin(9600); // Optional for debugging
11 }
12
13 void loop() {
14     // Main loop does nothing; I2C events are interrupt-driven
15 }
16
17 // Event handler for receiving data from the master
18 void receiveEvent(int bytes) {
19     while (Wire.available()) {
20         char c = Wire.read(); // Read each byte sent by the master
21         Serial.print("Received: ");
22         Serial.println(c); // Debug: Print received data
23     }
24 }
25
26 // Event handler for responding to master requests
27 void requestEvent() {
28     Wire.write(registerData); // Respond with the data in regist
29     Serial.print("Register 0x31 read, sending: ");
30     Serial.println(registerData, HEX);
31 }
```



Simulating the SDK





Vulnerability discovery - Final POC

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





Exploiting Over WiFi - Stack Overflow RCE

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



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.



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





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
D'y22

Moving to Cars





German
OWASP
Day 2-25

Moving to Cars

When you have limited budget





How do we connect to the device WiFi?







Agenda

01 **Intro to AirPlay, iAP2 and CarPlay**

02 **Vulnerability Discovery**

03 **Exploitation path to CarPlay**

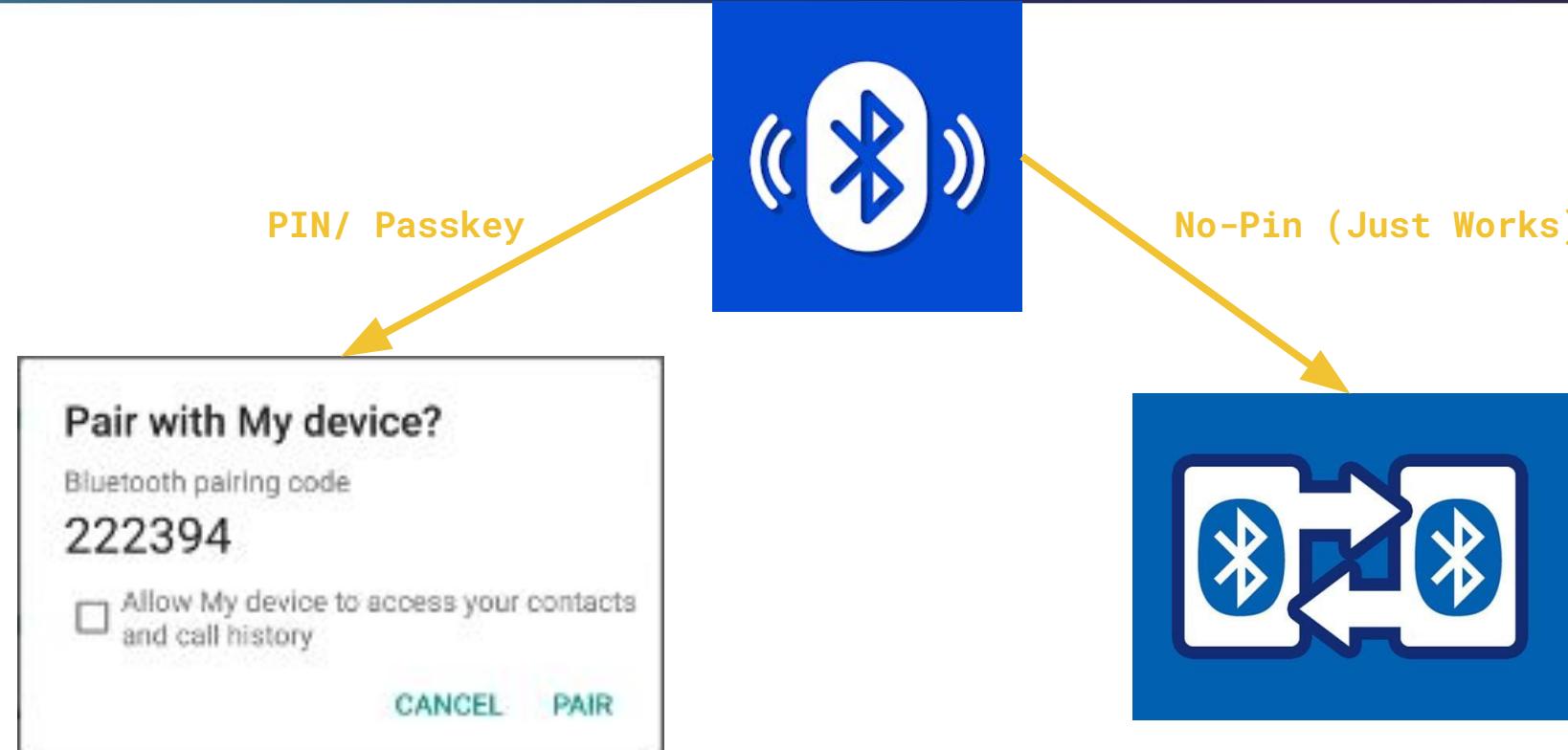
04 **iAP2 deep dive**

05 **Implications: supply chain & trust
in SDKs**

06 **Summary**



Bluetooth pairing





iAP2 Protocol Structure



iAP2



Apple CarPlay



iAP2 Packet Structure

Magic 1 (0xFF)	Byte 0
Magic 2 (0x5A)	Byte 1
Packet Length	Byte 2
Packet Length	Byte 3
SYN ACK EAK RST SUS 0 0 0	Byte 4
Packet Sequence Number	Byte 5
Packet Ack Number	Byte 6
Session ID	Byte 7
Header Checksum	Byte 8
Payload Data	Bytes 9 to X-1
Payload Checksum	Byte X



iAP2 Payload Structure

iAP2 Payload Structure

Magic 1 (0x40)

Byte 0

Magic 2 (0x40)

Byte 1

Payload Length

Byte 2

Payload Length

Byte 3

Payload

Byte 4 - end



iAP2 Checksum

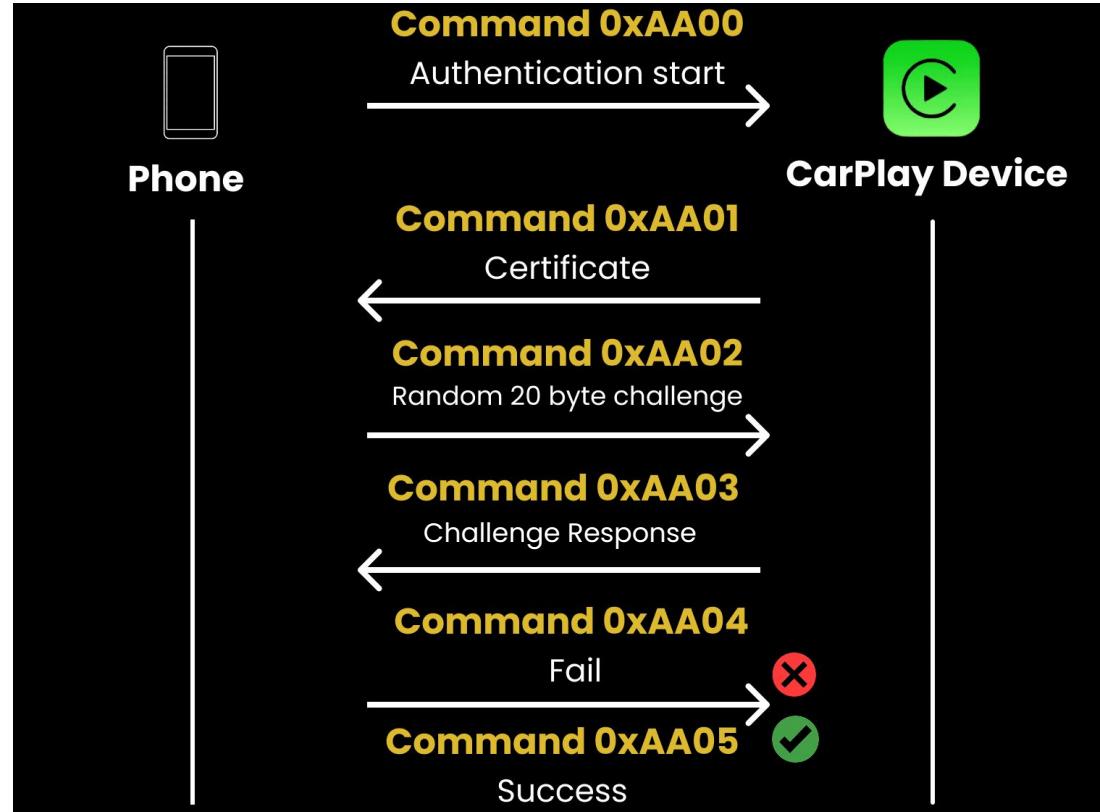
```
def iap2_calc_checksum(buffer: bytes) -> bytes: 2 usages
    if buffer and len(buffer) > 0:
        checksum = sum(buffer) & 0xFF
        checksum = (0x100 - checksum) & 0xFF
        checksum = struct.pack( fmt: "B", *v: checksum)
        return checksum
    else:
        print("Error: NULL buffer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



iAP2 Authentication

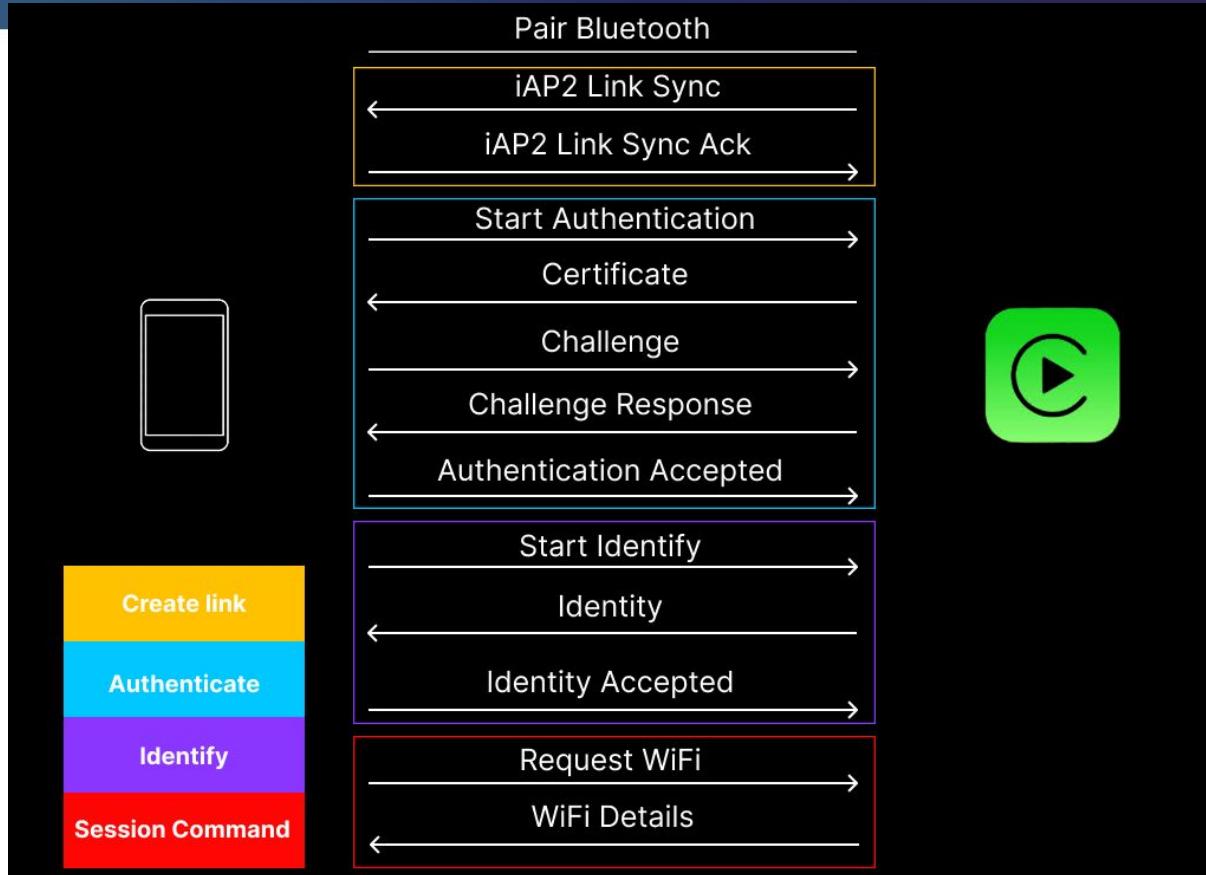
- Authentication is **one way**
- The phone authenticates the device
- The device **does not** authenticate the phone
- **Any device can impersonate a phone**

Authentication steps





iAP2 Session





iAP2 Wifi Credentials

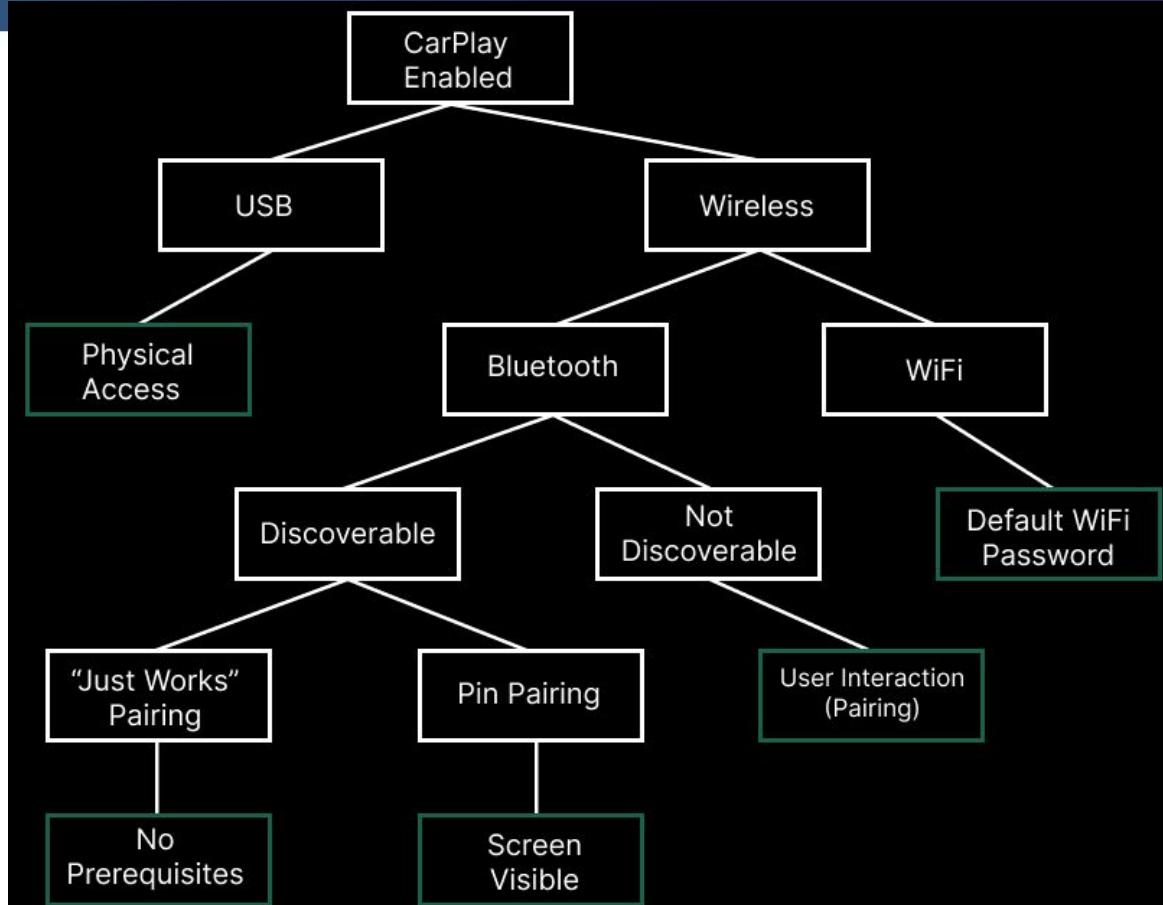
Container:



```
param_len = 5
param_id = 4
param_payload = b'\x95' (total 1)
```



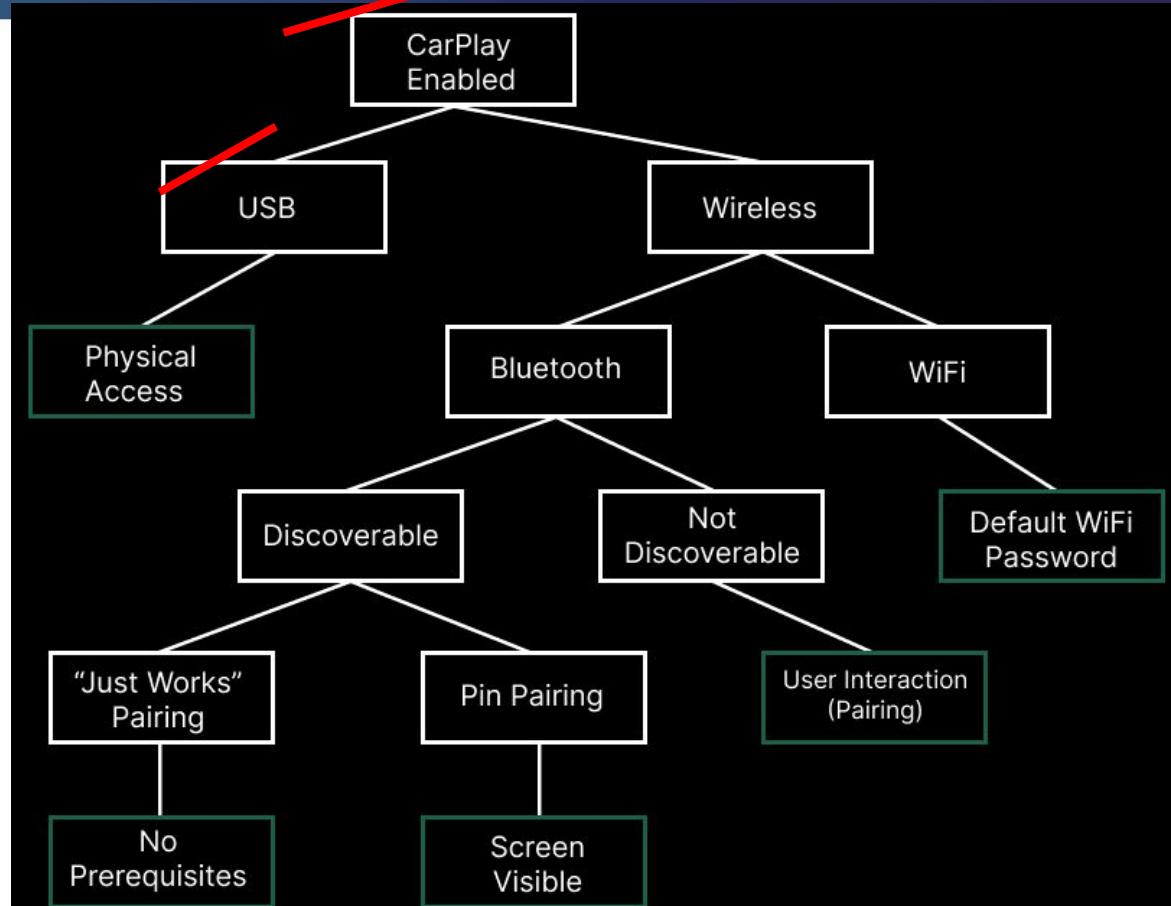
Prerequisites





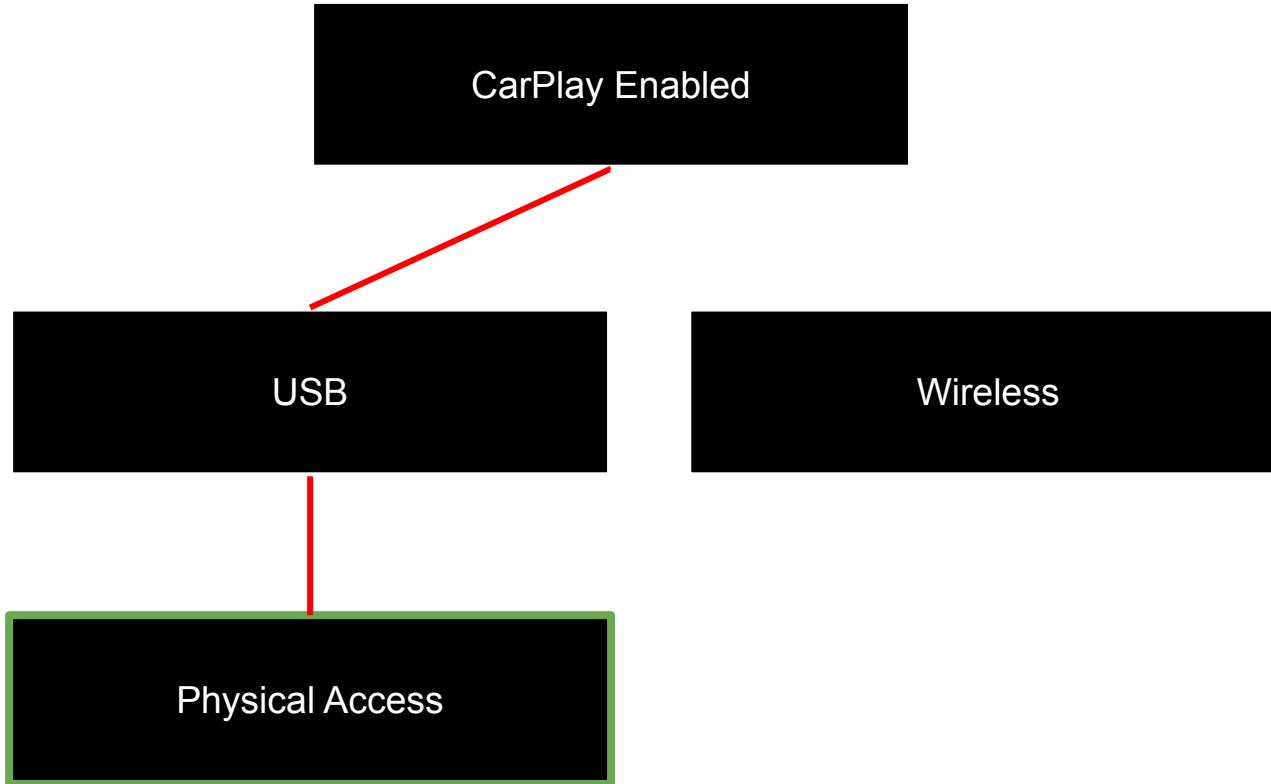
Prerequisites

1/5





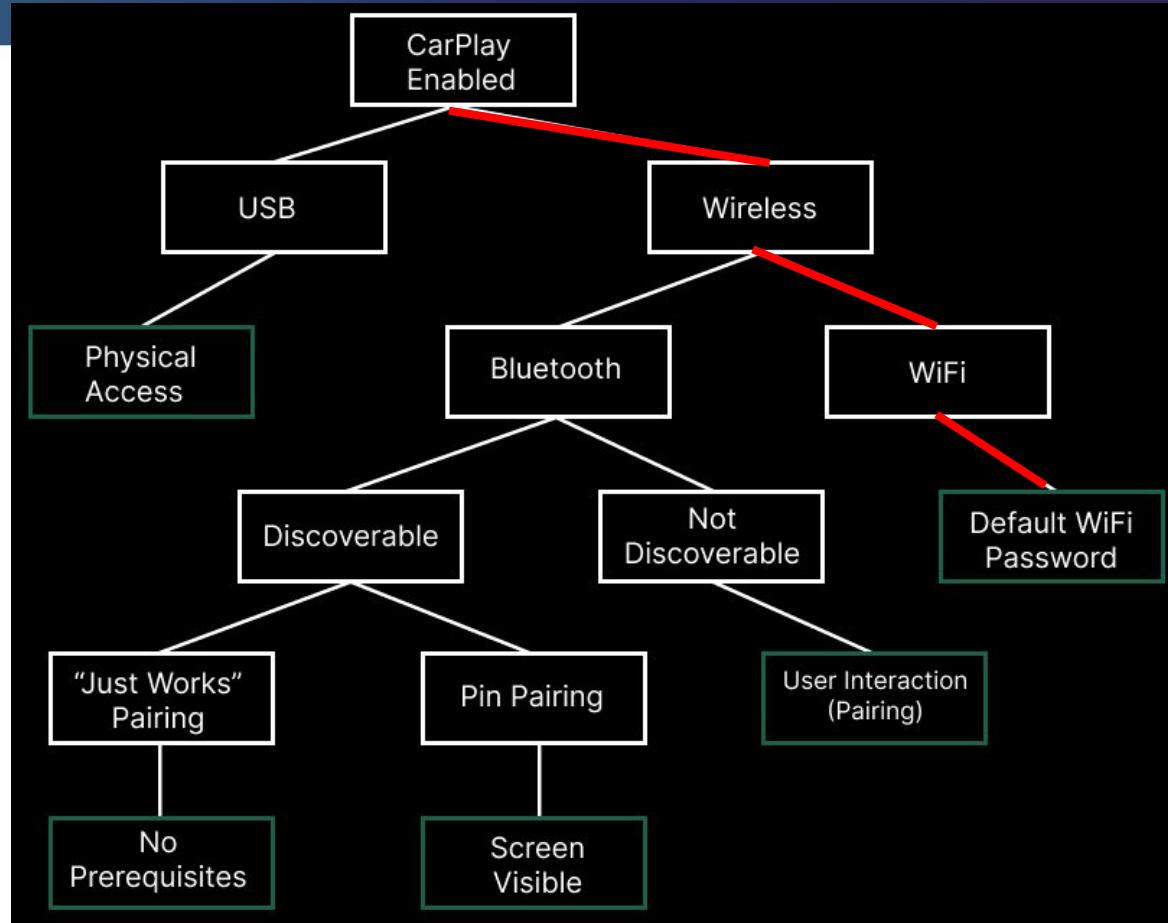
Prerequisites





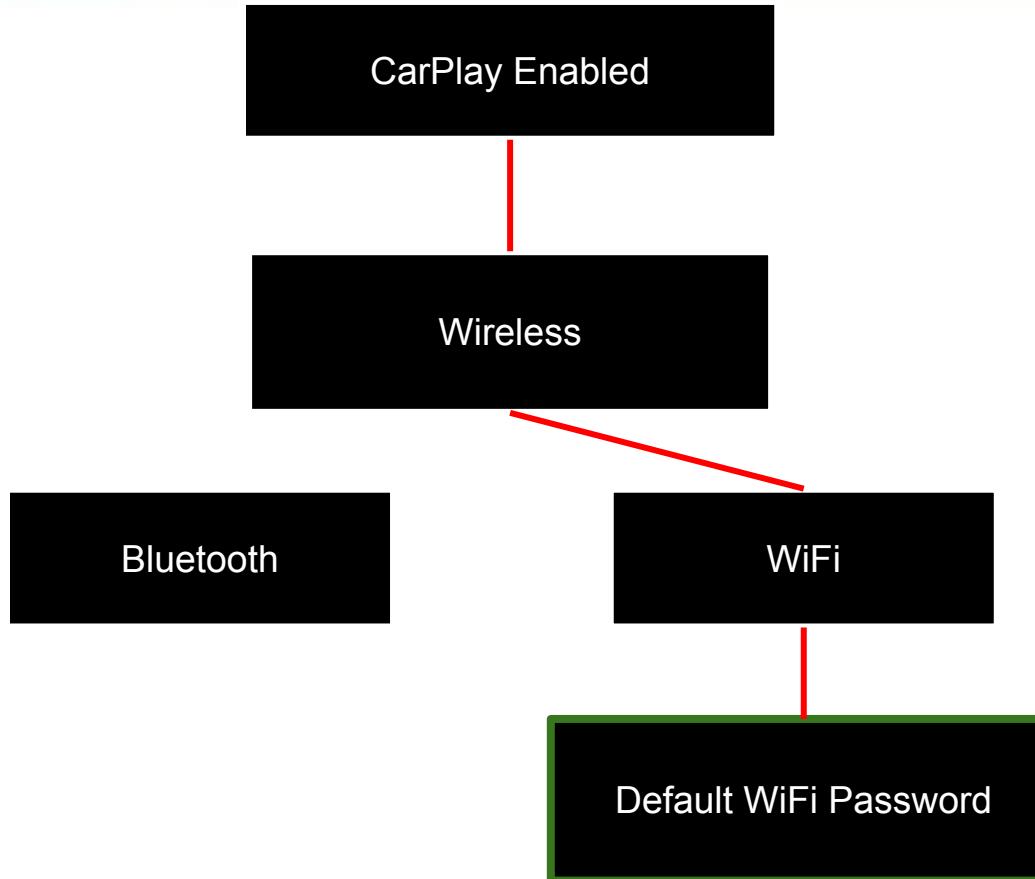
2/5

Prerequisites





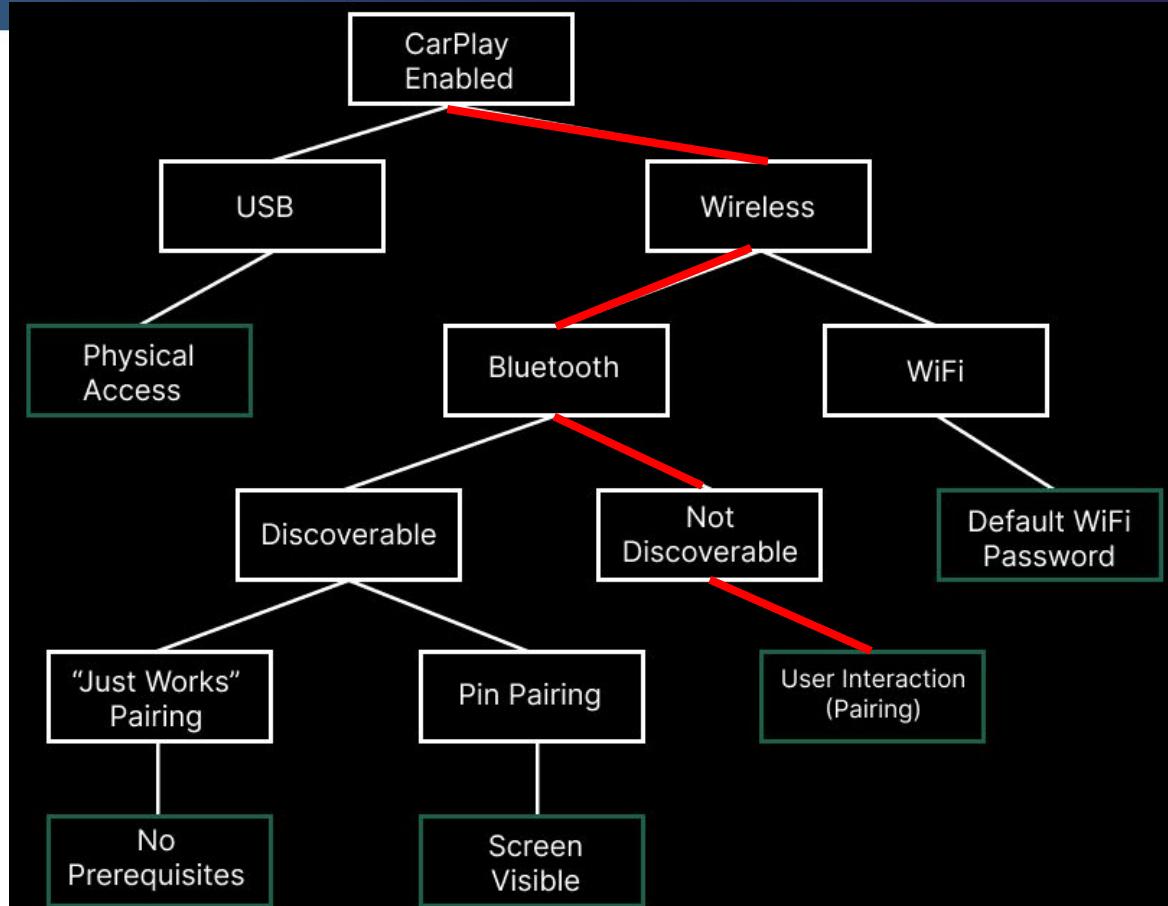
Prerequisites





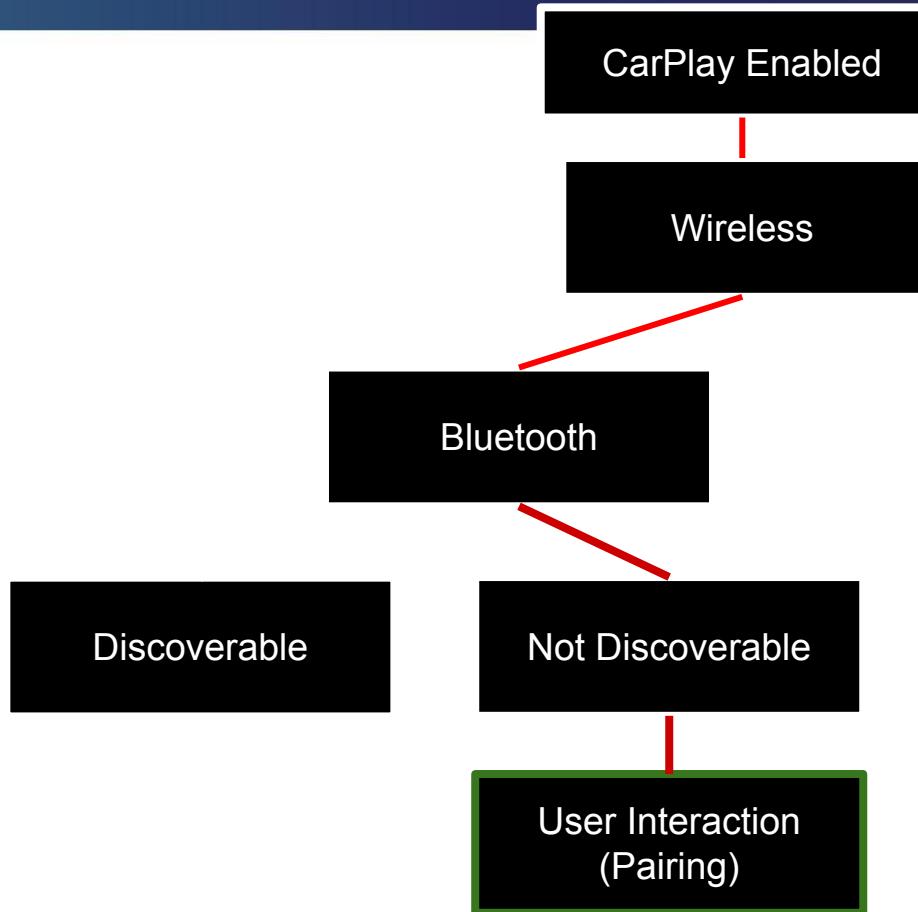
Prerequisites

3/5





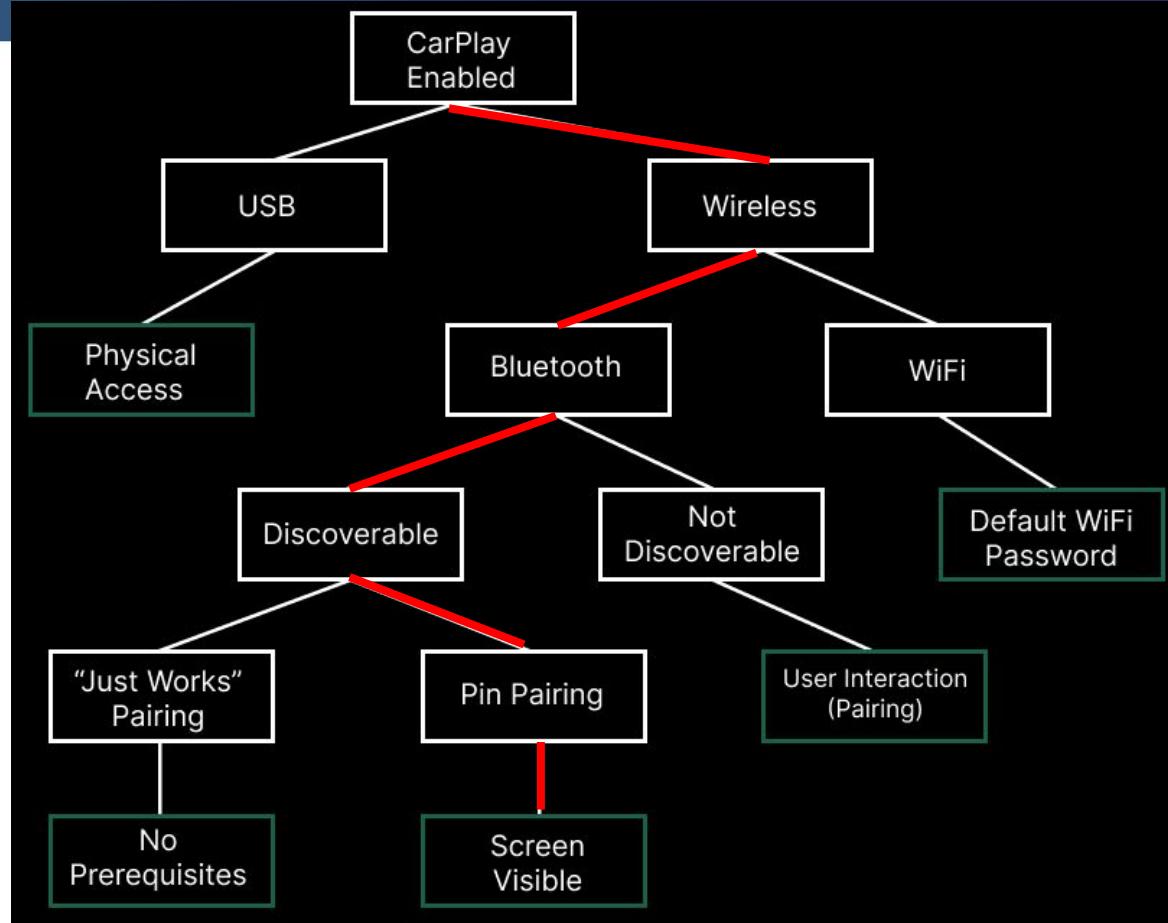
Prerequisites





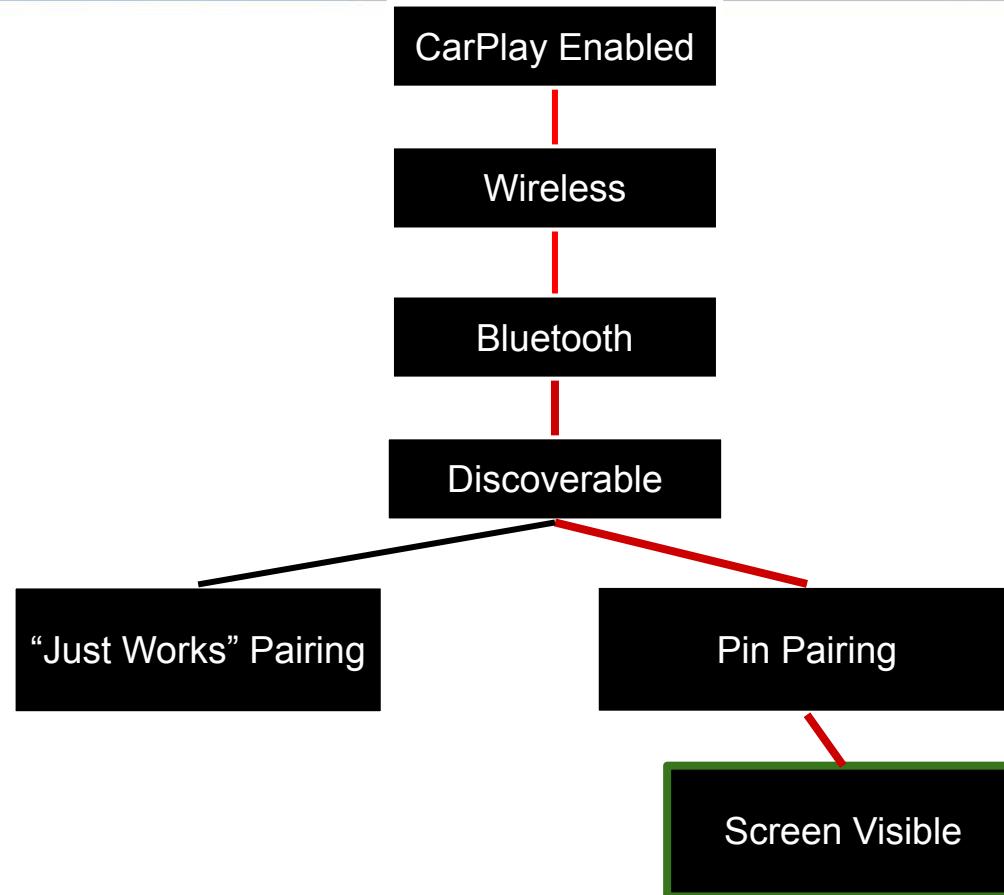
4/5

Prerequisites





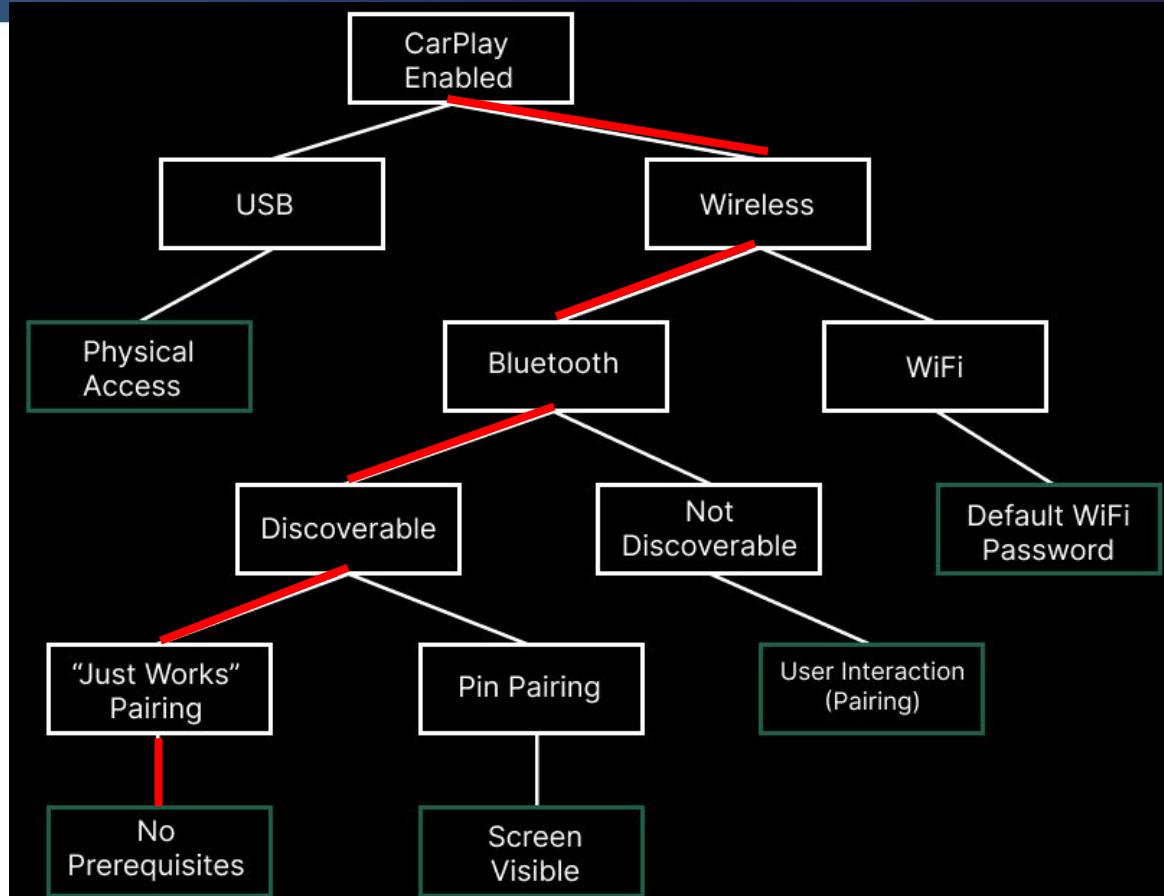
Prerequisites





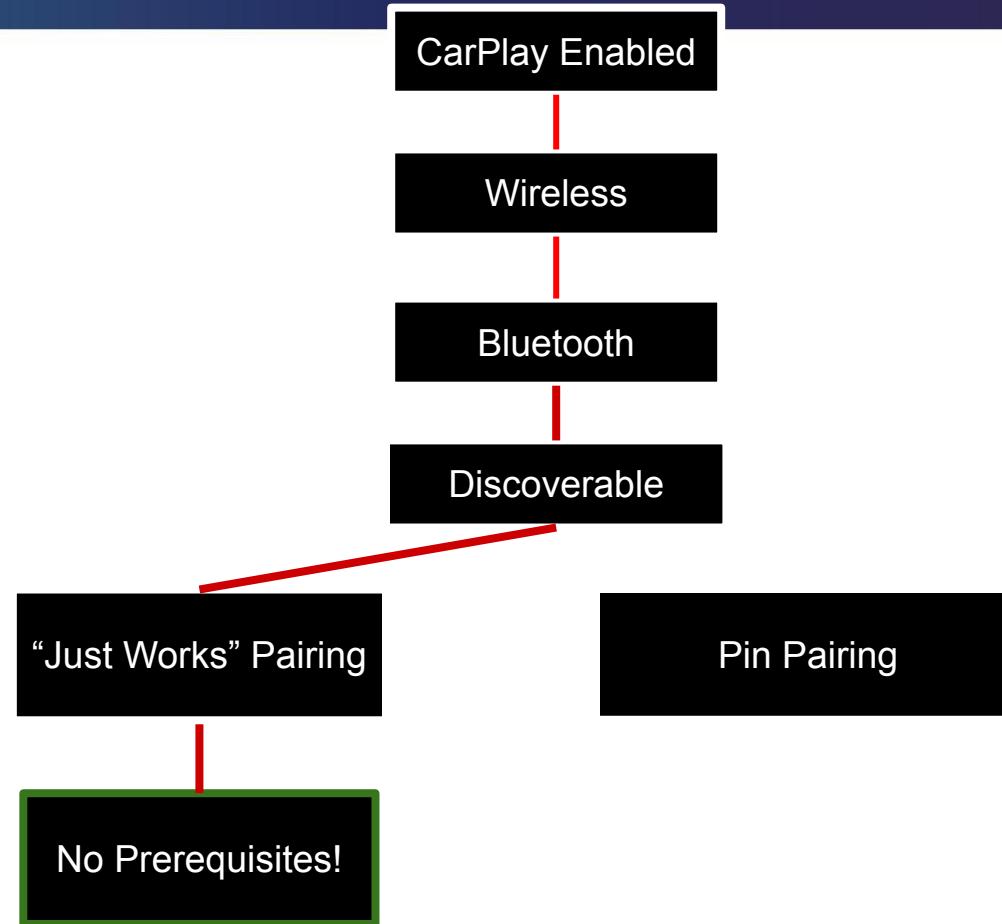
Prerequisites

5/5



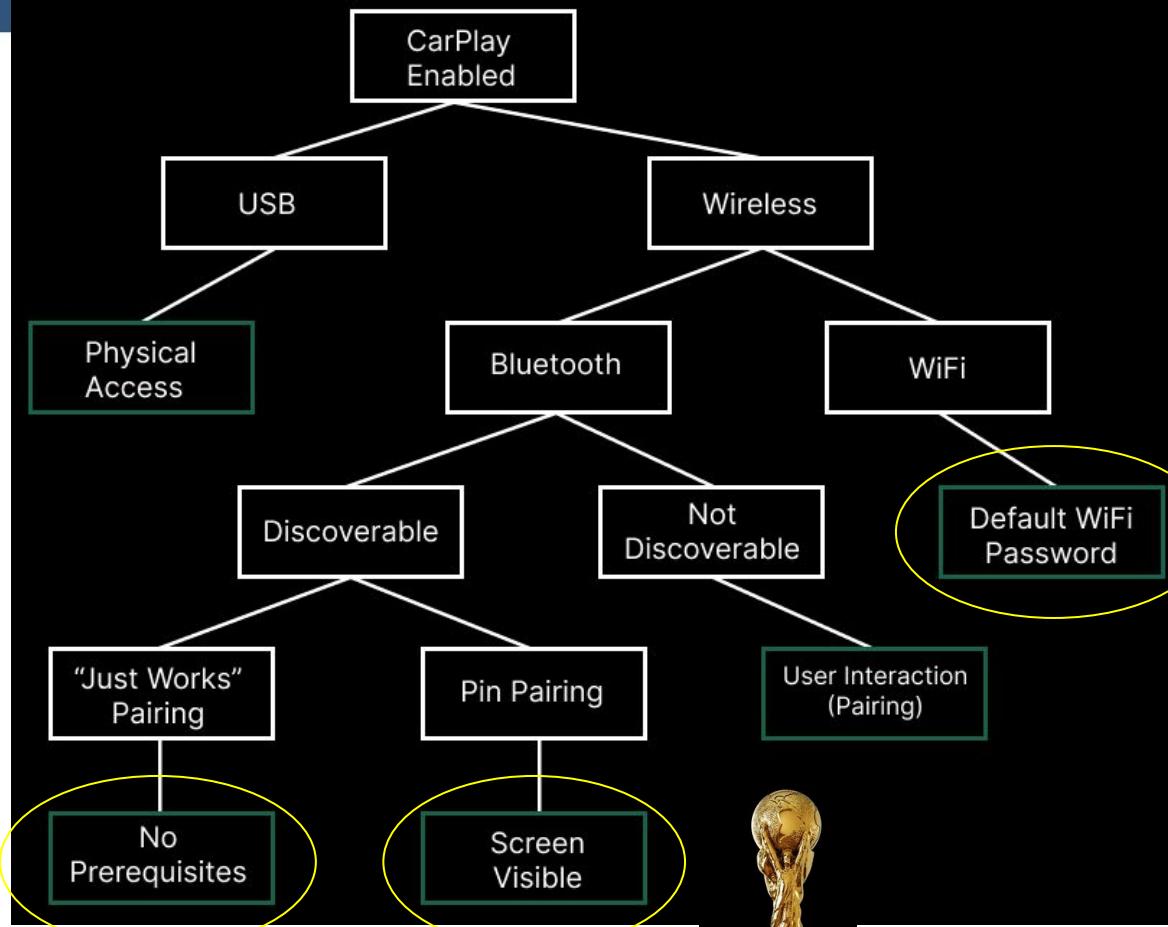


Prerequisites





Prerequisites





DEMO



AIRBORNE

CVE-2025-24132



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**



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



Agenda

01 **Intro to AirPlay, iAP2 and CarPlay**

02 **Vulnerability Discovery**

03 **Exploitation path to CarPlay**

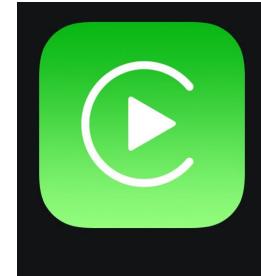
04 **iAP2 deep dive**

05 **Implications: supply chain & trust
in SDKs**

06 **Summary**



Summary





Questions?

*Pwn
My
Ride*





German
OWASP
Day 2025

Thank You!



Avi Lumelsky

avi@oligosecurity.io

[@avi_lum](https://twitter.com/avi_lum)



German
OWASP
Day 2025

THANK YOU!



German
OWASP
Day 2025



PRESENTATION TITLE
ON EVERYTHING
ABOUT
APPLICATION SECURITY
JONATHAN DAVIS III

01 TITLE OF THE FIRST GROUP OF SLIDES

SUB-HEADLINE



German
OWASP
Day 2025

THANK YOU!