Phone projection

20210638 최무송

Phone projection(Apple Carplay & Android Auto)

- Phone (mirroring) ➔ In-vehicle Infotainment display
  - Android Automotive: Android OS in vehicle

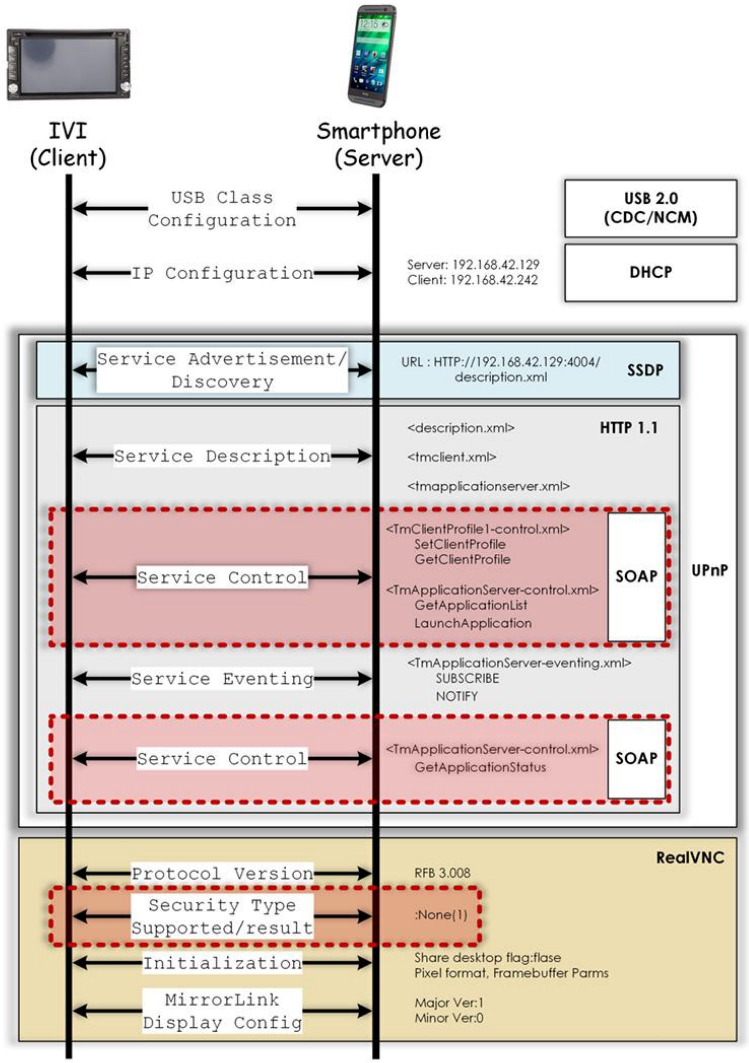
- Connected via USB cable / Wi-fi or Bluetooth

- Apps: GPS Navigation, Phone call, Message, Music player, …

- Minimized driver distraction
  - Voice command integration, simple UI, no media play when driving

MirrorLink

- MirrorLink vulnerabilities
  - DAP does not restrict untrusted devices
  - Heap overflow
  - Functions that can access to CAN bus
- Terminated in 2023



Apple Carplay components

- Apple Device (iPhone, adapter)
- Carplay Accessory (IVI)
- MFi(Made for iPhone/iPad/iPod) chip
  - Security and Authentication

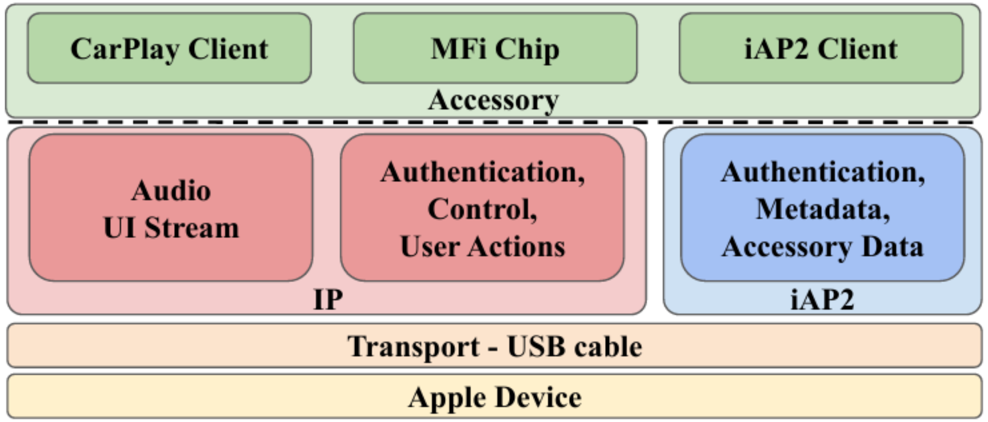


Figure 1: **CarPlay Overview.**

USB Connection between iPhone and IVI Systems

- USB connection (recognition)
- USB role switch
- iAP2(Inter-Accessory Protocol 2) session
  - Parameter negotiation
  - NCM configuration
  - IVI system Authentication
  - IVI system Identification
- CarPlay Session
  - IP Networking and Bonjour Discovery
  - CarPlay Session Authentication
  - Content Transfer and Application Launch

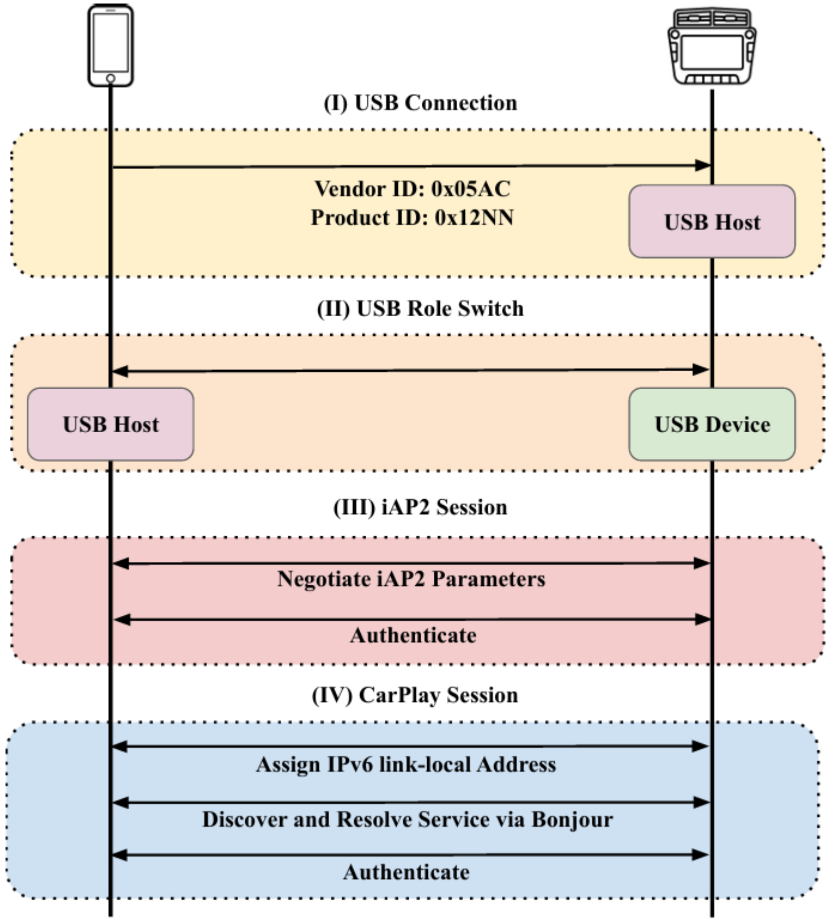
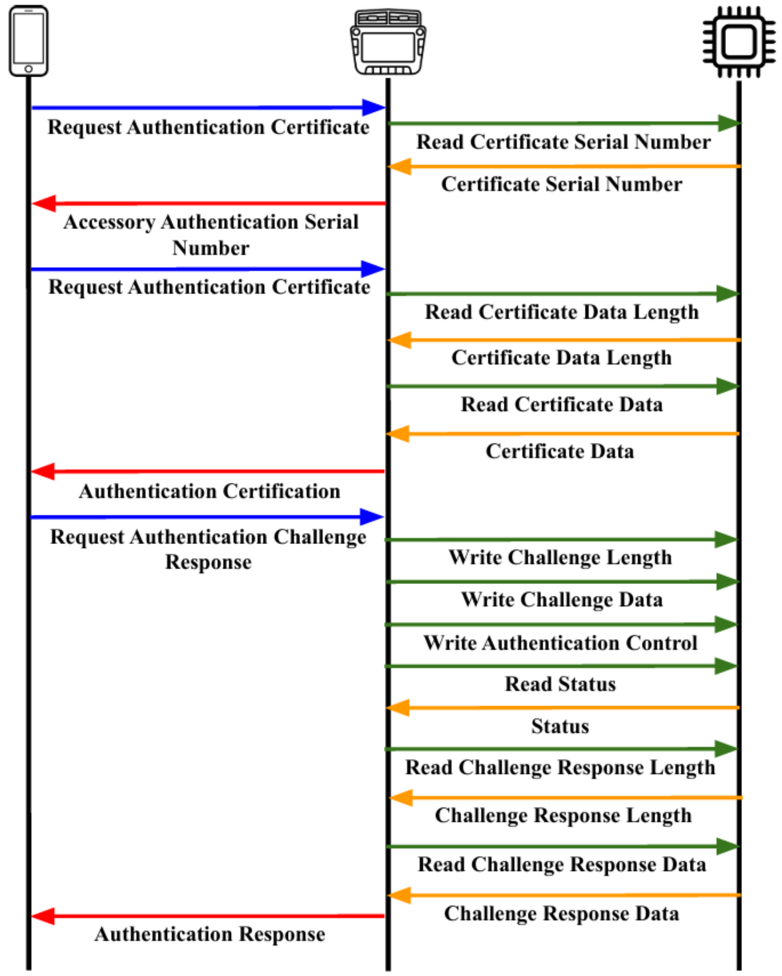


Figure 2: **Steps of Connection Establishment between iPhone and IVI Systems.**

IVI system Identification and Authentication

- Authorize accessories with Mfi chip



Request Authentication Certificate

Read Certificate Serial Number

Certificate Serial Number

Accessory Authentication Serial Number

Request Authentication Certificate

Read Certificate Data Length

Certificate Data Length

Read Certificate Data

Certificate Data

Authentication Certification

Request Authentication Challenge Response

Write Challenge Length

Write Challenge Data

Write Authentication Control

Read Status

Status

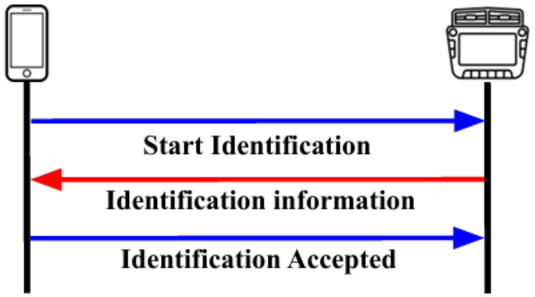
Read Challenge Response Length

Challenge Response Length

Read Challenge Response Data

Challenge Response Data

Authentication Response



Start Identification

Identification information

Identification Accepted

Packet Analysis (2025 paper)

- *The IVI system verifies only the product and vendor IDs from the USB descriptor to initiate the CarPlay session. Any device can easily forge these.*
- *However, contrary to the document's description, the authentication process does not include a packet requesting the serial number. Moreover, the identification process occurs prior to the authentication process in the iAP2 session.*

- By forging ID, Android OS can run within Carplay

Static Binary Analysis (2025 paper)

- *IVI systems are designed to accept any Apple device for CarPlay functionality without verifying whether the connected device is a genuine iPhone. Moreover, Apple assumes that only authorized iPhones will initiate CarPlay sessions, and therefore does not enforce an authentication mechanism on the IVI side.*

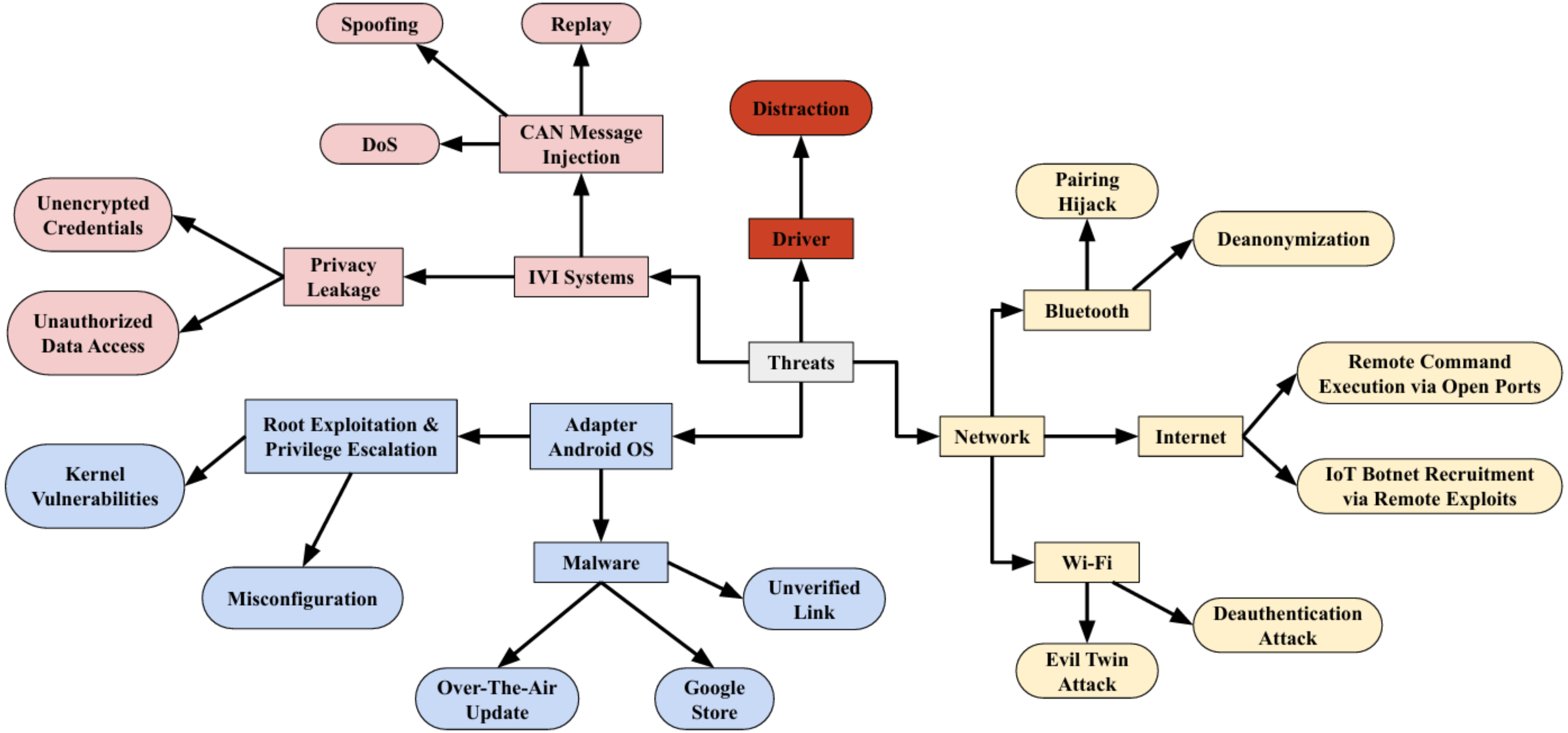
Julia Static Analysis (2018 paper)

- Android Auto는 플레이스토어에 등록된 앱만 사용 가능

- 앱 차원에서 보안 원칙을 위반하거나 (ex – Webview 사용으로 인한 XSS, javascript injection 가능성) Phone projection 규칙을 위반할 수 있음 (ex - 미디어 자동 재생 허용)

- *Results show that almost 80% of the apps are potentially vulnerable, out of which 25% poses security threats related to execution of JavaScript.*

Phone Projection Threats



References

- Vulnerability analysis of Android auto infotainment apps
- CarPlay at Risk: Unveiling Security Threats of Third-Party Infotainment Adapters
- A Security Analysis of an In Vehicle Infotainment and App Platform