Threat Analysis and Detection in In-Vehicle Infotainment System Leveraging MITRE ATT&CK

Yeonjae Kang and Huy Kang Kim, Korea University

2025. 08. 11

ABOUT ME

- Yeonjae Kang
- Now, PH.D course student in Korea University
- M.S. in Cybersecurity
- B.S. in Mathematics & Information Security (Double major)
- Key Expertise:

  Automotive Cybersecurity, Deep learning, Intrusion Detection

- Email: kangyj1995@korea.ac.kr



Introduction

In-Vehicle Infotainment systems : The Evolution of Risk & Critically

- The functions of In-Vehicle Infotainment (IVI) systems has evolved, making them **integral to autonomous vehicle operations**
- This evolution introduces new risks, as their data handling and connectivity **create a much wider attack surface**
- Research confirms that IVI exploits can **directly threaten safety by compromising vital controls** like braking and steering

Challenges in IVI Security Research

- **Limited access** due to proprietary E/E architectures and closed-source software
- **Difficulty setting up research environments** due to customized OS structures
- **Presence of unique constraints** distinct from traditional IT security

Ethical Considerations

- Designed to prevent any harm to the driver or physical vehicle systems
- Prioritizes the protection of personal data and the maintenance of system integrity
- Emphasizes academic and industrial contributions to enhancing vehicle security

Contributions:

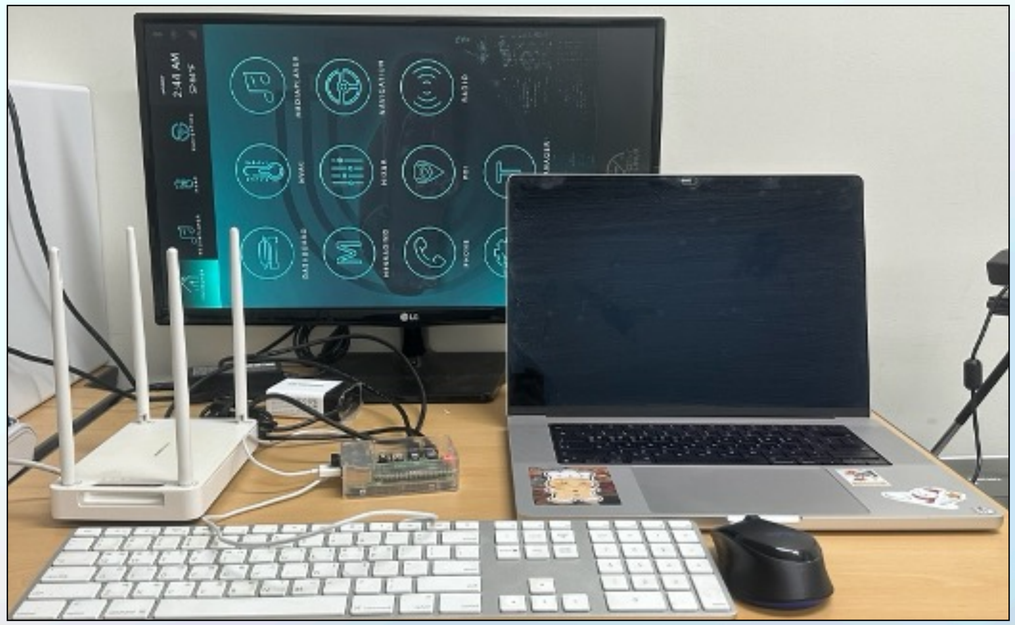
- Design and Implementation of IVI Attack Scenarios
- Classification and Analysis Using MITRE ATT&CK
- Design of Multiple-phase Attack Sequences
- Rule-Based Detection

Experimental Setup

IVI Testbed Initialization

An IVI testbed was built to simulate a real-world environment using Automotive Grade Linux (AGL)

- Platform:
  - AGL v12.1.3 (Lucky Lamprey)
  - Compiled for and deployed on a Raspberry pi 4
- Testbed Components:
  - Hardware: Raspberry Pi 4, I/O devices, router, attacker PC
  - Interfaces:
    - Physical (6): Wi-Fi, Ethernet, Bluetooth, USB, GPIO, MicroSD
    - Logical (2): Human-Machine Interface (HMI), Virtual CAN



Key Advantages of the Testbed Environment

- **Realism**: Simulates the resource-constrained nature of an actual production vehicle
- **Versatility**: Capable of executing a wide range of attack vector
- **Practicality**: Offers a balanced environment that is both controllable for research and realistic for valid security evaluations

Vulnerability Analysis

- Absence of authentication and encryption in Inter-Process Communication (IPC)
- Allows attackers to manipulate JSON messages exchanged between IVI applications and services
- Impact
  - Enable theft and forgery of configuration data
  - Leads to malfunction of critical system functions
- Primary Attack Vector
  - Wi-Fi and Ethernet interfaces
  - **CVE-2022-24595**

Assumed Attacker Profile (Threat Model)

- **Access**: Has gained initial access to the internal system
- **Knowledge**: Possesses a clear understanding of the network and system architecture
- **Capability**: Equipped with advanced penetration testing skills

Attack Scenarios and Classifications

Target Scope & Analysis Methodology

- Applications: Entire System, Navigation, Phone, Messaging, HVAC, Mediaplayer
- Priority: Core functionalities with significant user interaction
- MITRE ATT&CK Mapping (v16.1): Identifying adversary tactics and techniques
- Impact-Based Classification

Classification 1 : Reconnaissance

Initial Attack Phase: The First Step of an Attack

- Information Gathering: The core activity of this initial phase. Attackers collect vital data on targets like systems, networks, and users
- Vulnerability Identification: The primary goal is to discover exploitable weaknesses
- Strategic Foundation: This stage is essential for planning and launching a successful, full-scale attack

Attack Scenario #1: Port Scanning

Reconnaissance

Tactics	Reconnaissance (TA0043)
Techniques	Active Scanning (T1595)
	Gather Victim Information (T159

TCP port	Process
30031	afbd-dashboard
30032	afbd-homescreen
30033	afbd-hvac
30034	afbd-launcher
30035	afbd-mediaplayer
30036	afbd-messaging
30037	afbd-mixer
30038	afbd-navigation
30039	afbd-phone
30041	afbd-radio
30042	afbd-settings
30043	afbd-taskmanager

- SYN packets were sent to all 1–65,535 ports on the AGL server
- 37 open and accessible ports were identified along with their corresponding processes

Classification 2: Exfiltration

Information Theft Attack Scenarios

- Primary Objective: To gain unauthorized access and exfiltrate sensitive system information
- Common Methods: Includes network traffic interception, exploitation of Application Programming Interfaces (APIs), and taking advantage of was data access controls, etc

Attack Scenario #2: Location Data Exfiltration

Exfiltration

Tactics	Collection (TA0043) & Exfiltration (TA0010)
Techniques	Application Layer Protocol (T1071)
	Data From Local System (T1005)
	Automated Collection (T1119)

- Attacker exploits a legitimate navigation API to extract the real-time vehicle location
- By using the “subscribe” verb, attacker accesses the vehicle’s current position without authentication or user awareness

Attack Scenario #3: Phone Data Exfiltration

Exfiltration

Tactics	Collection (TA0043) & Exfiltration (TA0010)
Techniques	Exfiltration Over Bluetooth (T1011.001)
	Data from Removable Media (T1025)
	Automated Collection (T1119)

- Attacker illegally collect a connected device's phonebook and recent call history by exploiting the bluetooth_pap API

Attack Scenario #4: Message Logs Exfiltration

Exfiltration

Tactics	Collection (TA0043) & Exfiltration (TA0010)
Techniques	Exfiltration Over Bluetooth (T1011.001)
	Data from Removable Media (T1025)
	Automated Collection (T1119)

- Attacker exploit the bluetooth_map API by using the list_messages verbs to extract message data from the paired device
- Attacker specifies a target folder using the folder variable
- By iterating through each folder, attacker can systematically steal the entire message list from the connected device

Classification 3: Manipulation

System Disruption Attack scenarios

- Attack Category: Encompasses various scenarios where an attacker disrupts the normal functionality of the In-Vehicle Infotainment (IVI) system
- Execution Method: The attacker manipulates system behavior, either directly or through remote control, to perform malicious actions or induce the execution of malicious commands

Attack Scenario #5: HVAC Control Spoofing

Manipulation

Tactics	Execution (TA0002) & Impact (TA0040)
Techniques	System Services (T1569)
	Create or Modify System Process (T1543)

- Attacker send well-crafted packets to arbitrarily adjust the vehicle's temperature and fan speed
- By exploiting the set verb of the HVAC API, attacker can gain control over the vehicle's HVAC system
- This scenario generates CAN messages that are transmitted from the IVI system to the in-vehicle network

Attack Scenario #6: Navigation Destination Spoofing

Manipulation

Tactics	Execution (TA0002) & Impact (TA0040)
Techniques	System Services (T1569)
	Create or Modify System Process (T1543)

- The vulnerability lies in the sequential execution of the broadcast_waypoints( ) and broadcast( ) functions
- Attacker manipulates the input fields for latitude and longitude
- The system is redirected to an arbitrary location chosen by attacker

Attack Scenario #7: Message Sending Spoofing

Manipulation

Tactics	Impact (TA0040) & Command and Control (TA0011)
Techniques	Remote Access Software (T1219)
	Hijack Execution Flow (T1574)
	Application Layer Protocol (T1071)

- Attacker exploits the compose verb of the Bluetooth MAP API
- The compose function creates a structured message format called bMessage, which is essential for Bluetooth MAP

Attack Scenario #8: Phone Dialing Spoofing

Manipulation

Tactics	Impact (TA0040) & Command and Control (TA0011)
Techniques	Remote Access Software (T1219)
	Hijack Execution Flow (T1574)
	Application Layer Protocol (T1071)

- Attacker exploits a vulnerability in the Telephony API, which includes dial( ) and hang up( ) functions
- Attacker tricks the IVI system into making calls to specific malicious numbers without the driver's knowledge or consent

Classification 4: Redirection

Malicious Redirection: Altering Data and Misleading Users

- Core Tactics: This classification includes various tactics where an attack redirects users to unintended, potentially harmful resources or modifies legitimate data for illicit purposes
- Key Examples: Representative attacks in this category include Man-in-the-Middle (MITM), DNS spoofing, and API response tampering, etc

Attack Scenario #9: Navigation Map Pharming

Redirection

Tactics	Initial Access (TA0001) & Impact (TA0040)
Techniques	Adversary-in-the-Middle (T1557)
	Hijack Execution Flow (T1574)

- This scenario leverages a key vulnerability when the navigation API fails to respond
- Attacker uses techniques like ARP spoofing and fake DNS attacks to redirect the domain's IP address to an HTTP server they control

Classification 5: DoS

Undermining Stability and Causing Service Denial

- Core Scenario: Includes scenarios where an attacker intentionally attempts to disrupt normal system operations
- Primary Impact: Degrades the stability of the IVI system, often leading to a Denial of Service condition

Attack Scenario #10: Mediaplayer POST Flooding

Tactics	Impact (TA0040)
Techniques	Network Denial of Service (T1498)
	Resource Hijacking (T1496)
	Endpoint Denial of Service (T1499)

- Attacker exploits a vulnerability in the Mediaplayer app's memory management
- Attacker sends a series of large HTTP POST messages, each approximately 32 KB in size

DOS

Attack Scenario #1 1: Message Payload DoS

Tactics	Impact (TA0040)
Techniques	Endpoint Denial of Service (T1499)
	Application or System Exploitation (T1499.004)

- Attacker sends a well-crafted, malformed JSON payload to the Messaging app
- The payload is structured as {“key”: “veryLongData…”}
- The excessively long data string is designed to cause a memory exhaustion exception

DoS

Multi-phase Attack Sequences

Multiple-phase Attack Sequence ?

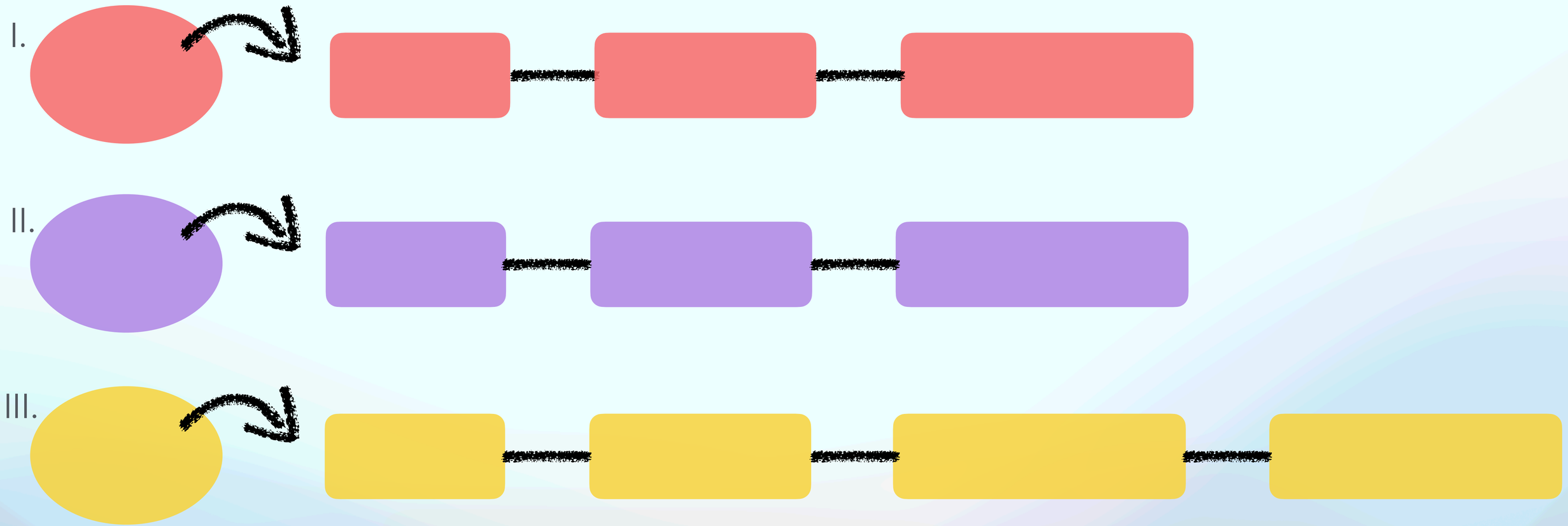
- Our research utilizes a series of attack scenarios designed to be executed in a logical progression
- These are structured as a cohesive attack sequence, which enhances real-world applicability and demonstrates a higher overall risk
- The sequence integrates individual scenarios targeting the Navigation, Messaging, and Phone applications

Target

I.

II.

III.



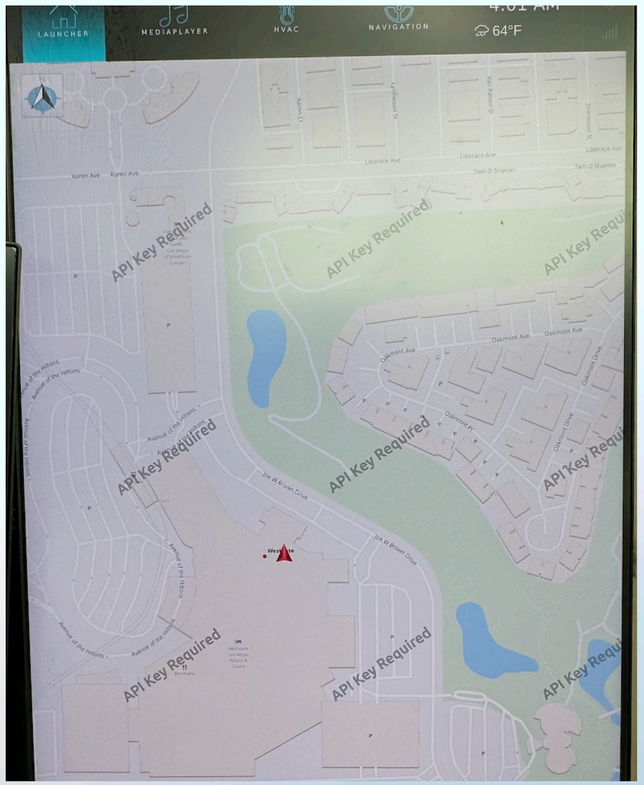
Multi-phase Attack Sequence 1

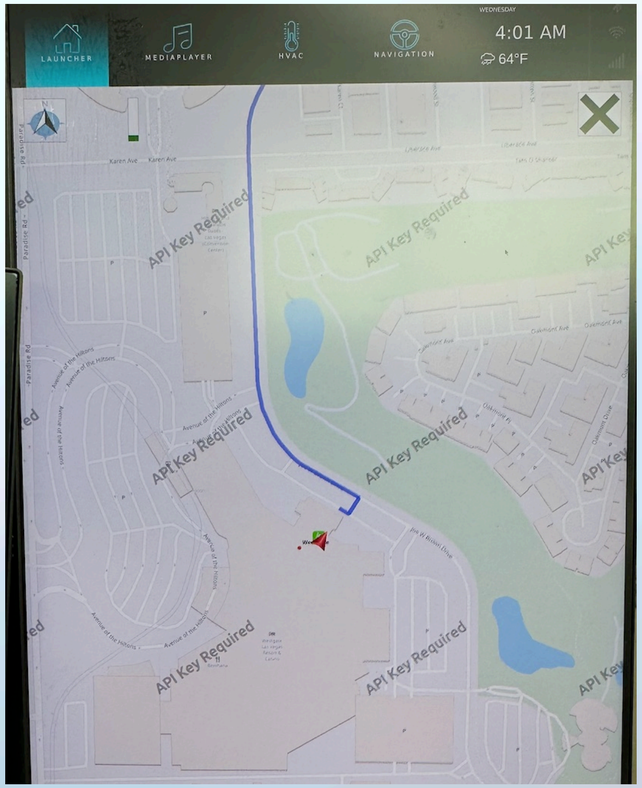
Port Scanning → Location Data Exfiltration → Navigation Destination Spoofing

- Attacker scans the IVI system to identify services related to the Navigation App
- Real-time GPS data is silently extracted
- Destination is silently modified without user consent
- Potential Consequences:
  - Location-based stalking, vehicle theft, etc…

```
-- Running: Location Data Exfiltration Attack --
->> Current Location: [latitude, logitude] = [36.1363 ° N, -115.151 ° N]
```

```
-- Running: Navigation Destination Spoofing Attack --
->> Set the Malicious Destination: [36.136852204258616 ° N, -110.15215351750138 ° N]
->> Set the Malicious Destination: [36.136852204258616 ° N, -112.1526338596952 ° N]
->> Set the Malicious Destination: [35.4283123 ° N, -115.15225803984872 ° N]
->> Set the Malicious Destination: [35.4283123 ° N, -115.15003782038569 ° N]
->> Set the Malicious Destination: [36.13471439613639 ° N, -115.15003782038569 ° N]
->> Set the Malicious Destination: [31.2394441 ° N, -115.15225803984872 ° N]
->> Set the Malicious Destination: [35.4283123 ° N, -110.15215351750138 ° N]
->> Set the Malicious Destination: [36.13471439613639 ° N, -110.15215351750138 ° N]
->> Set the Malicious Destination: [35.4283123 ° N, -115.15003782038569 ° N]
->> Set the Malicious Destination: [31.2394441 ° N, -112.1526338596952 ° N]
```





Multi-phase Attack Sequence 2

Port Scanning — Phone Data Exfiltration — Phone Dialing Spoofing

- Attacker scans the IVI system to identify active services and ports associated with the Phone App
- Contacts and call logs are extracted from the smartphone connected via Bluetooth
- Attacker manipulates the IVI system to place calls to arbitrary numbers
- Potential Consequences:
  - Identity theft / phishing, financial loss via unauthorized premium calls, etc…

```
-- Running: Phone Data Exfiltration Attack --
[Phone Book Data]
->> # Name: TEST 1, Number: 010[redacted]5678

->> # Name: TEST 2, Number: 010[redacted]6789

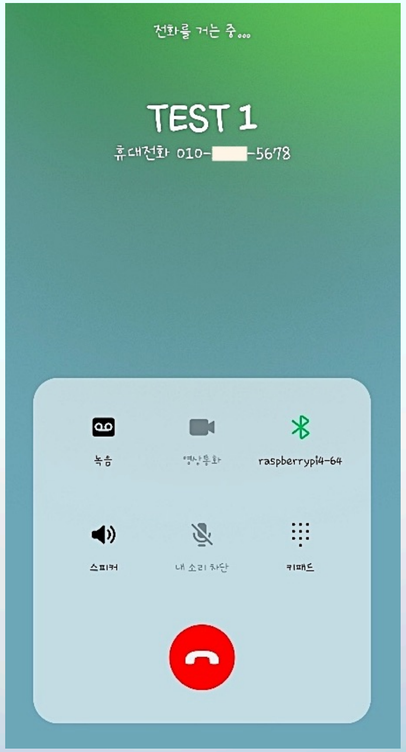
->> # Name: TEST 3, Number: 010[redacted]7890

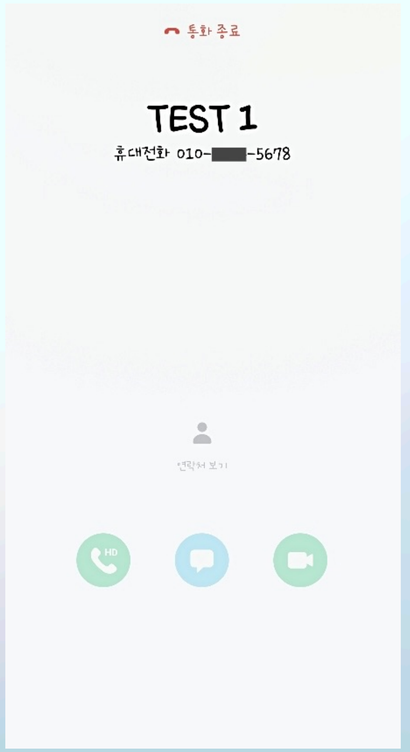
->> # Name: TEST 4, Number: 010[redacted]8901

->> # Name: TEST 5, Number: 010[redacted]2222

[Recent Call Logs]
->> # Name: UNKNOWN, Number: 010[redacted]2568
->> # Name: TEST 1, Number: 010[redacted]5678
->> # Name: TEST 4, Number: 010[redacted]8901
->> # Name: TEST 3, Number: 010[redacted]7890
->> # Name: TEST 5, Number: 010[redacted]2222
->> # Name: TEST 3, Number: 010[redacted]7890
->> # Name: TEST 1, Number: 010[redacted]5678
->> # Name: TEST 5, Number: 010[redacted]2222
```

```
-- Running: Phone Dialing Spoofing Attack --
->> Our Target: 010[redacted]2521
->> Dial to 010[redacted]2521
->> Our Target: 010[redacted]2521
->> Dial to 010[redacted]2521
```





Multi-phase Attack Sequence 3

Port Scanning → Message Logs Exfiltration → Message Sending Spoofing → Message Payload DoS

- Attacker identifies open services and APIs associated with the Messaging App
- Extracts recent messages from the smartphone via the IVI system
- Attacker sends spoofed messages to arbitrary recipients using the victim's device
- Injects malformed payloads to crash the messaging service
- Potential Consequences:
  - Phishing, tampering with communication channels, etc…

```
-- Running: Phone Data Exfiltration Attack --
[Phone Book Data]
->> # Name: TEST 1, Number: 010[redacted]5678

->> # Name: TEST 2, Number: 010[redacted]6789

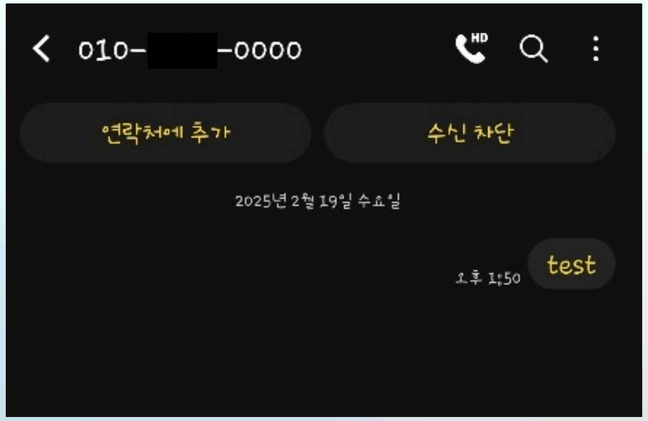
->> # Name: TEST 3, Number: 010[redacted]7890

->> # Name: TEST 4, Number: 010[redacted]8901

->> # Name: TEST 5, Number: 010[redacted]2222

[Recent Call Logs]
->> # Name: UNKNOWN, Number: 010[redacted]2568
->> # Name: TEST 1, Number: 010[redacted]5678
->> # Name: TEST 4, Number: 010[redacted]8901
->> # Name: TEST 3, Number: 010[redacted]7890
->> # Name: TEST 5, Number: 010[redacted]2222
->> # Name: TEST 3, Number: 010[redacted]7890
->> # Name: TEST 1, Number: 010[redacted]5678
->> # Name: TEST 5, Number: 010[redacted]2222
```

```
-- Running: Phone Dialing Spoofing Attack --
->> Our Target: 010[redacted]2521
->> Dial to 010[redacted]2521
->> Our Target: 010[redacted]2521
->> Dial to 010[redacted]2521
```



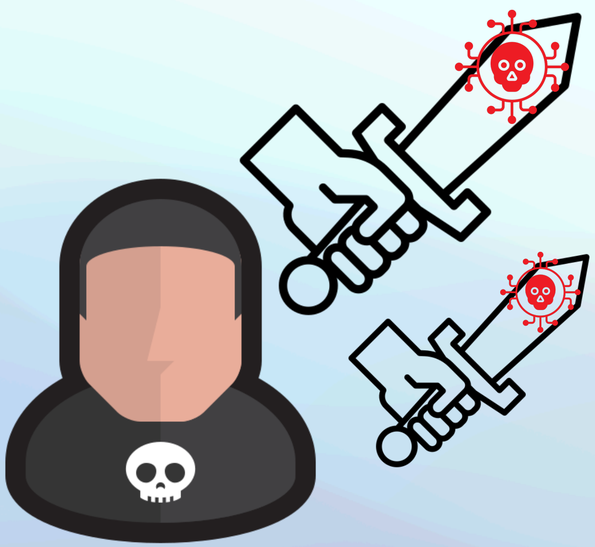

```
raspberrypi4-64:~# ps aux | grep 30036
root         727  0.0  0.0   2744   628 pts/0    S+   04:02   0:00 grep 30036
raspberrypi4-64:~#
```

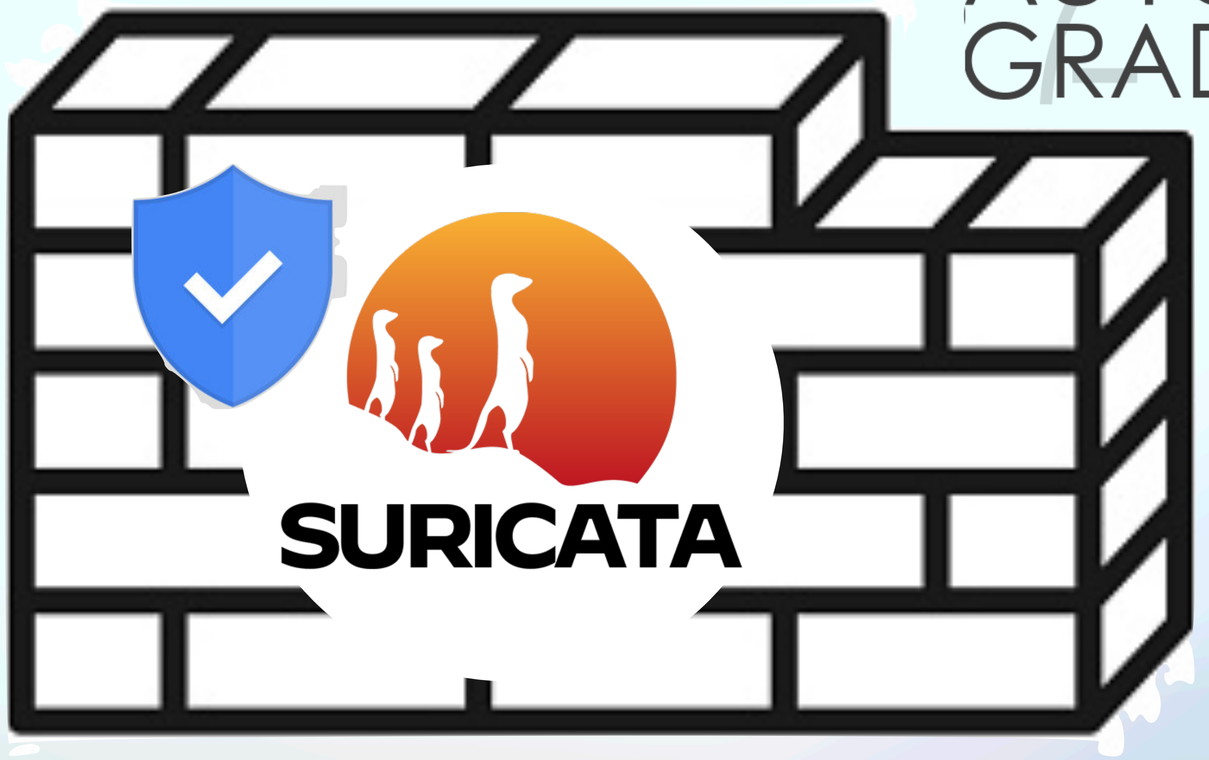
```
raspberrypi4-64:~# ps aux | grep 30036
agl-dri+     710 21.6  0.8 371588 70348 ?        Sl   03:51   0:01 /var/local/
lib/afm/applications/messaging/bin/messaging 30036 @t
root         715  0.0  0.0   2744   644 pts/0    S+   03:51   0:00 grep 30036
raspberrypi4-64:~#
```

Intrusion Detection with Suricata

Suricata on AGL

*Automotive Grade Linux





AUTOMOTIVE GRADE LINUX

Suricata Rule for Port Scanning Attack

★ Key Concept for Detection: SYN Packet Volume

- Normal Behavior: Characterized by standard network management traffic, such as IGMP for subnet management and SSDP for service discovery
- Attack Behavior: Indicated by a significant and abnormal surge in SYN packets, which is a key indicator of a SYN flood attack
- Detection Rule Logic
  - Packet Filtering: A flag (e.g., the 's' option) is used to specifically isolate and count packets with the SYN flag set
  - Threshold Mechanism: A rate-limiting threshold defines the maximum number of SYN packets permitted per second before an alert is triggered

Suricata Rule for Phone Dialing Spoofing Attack

★ Key Concept for Detection: FIN & ACK Packets in TCP

- Normal Behavior: Session established once and maintained until AGL termination. FIN & ACK packets occur once
- Attack Behavior: Repeated session termination and re-establishment. Triggers abnormal bursts of FIN & ACK packets
- Detection Rule Logic
  - Packet Filtering: Only capture packets TCP FIN(F) or ACK(A) flags
  - Threshold Mechanism: Define a limit for the number of FIN & ACK packets within a 1-second interval

Suricata Rule for Navigation Map Pharming Attack

★ Key Concept for Detection: ARP packets

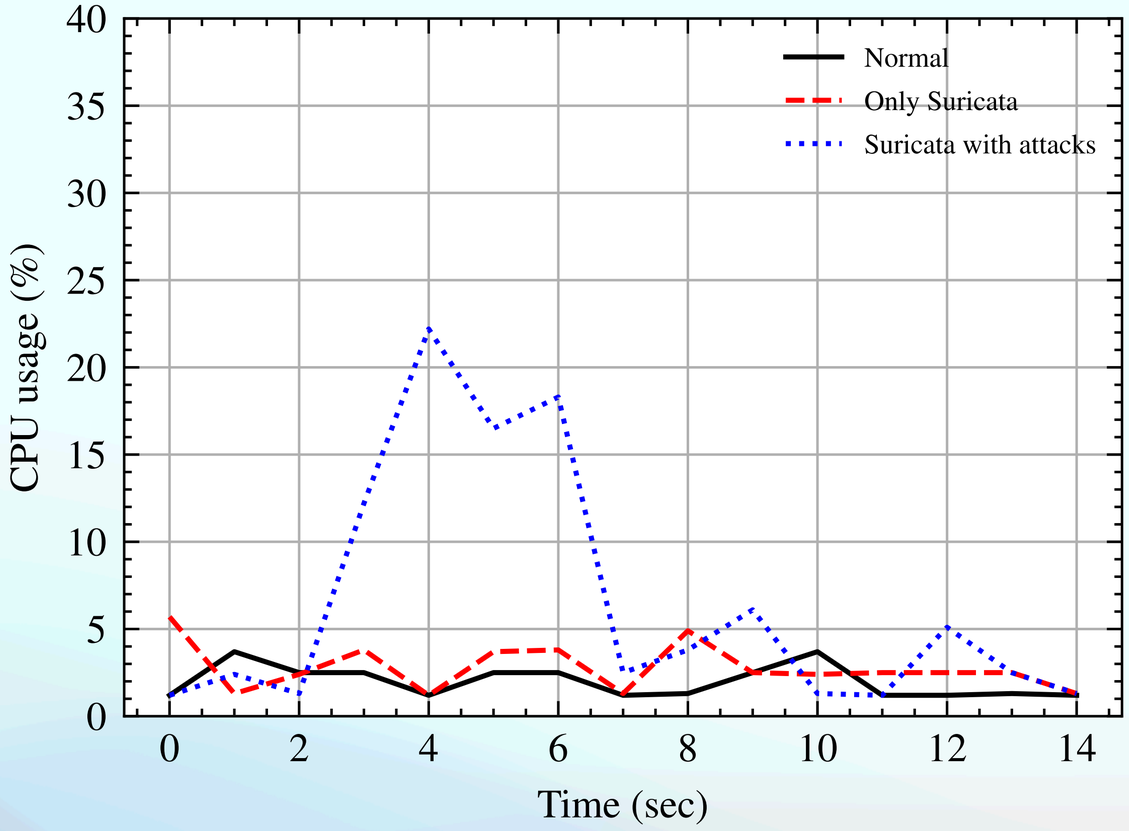
- Limitation: Suricata's native support
  - Suricata does not natively support ARP packet filtering
  - Requires use of raw packet matching for ARP detection
- Detection Rule Logic
  - Content Option: Detect Ethernet Type field for ARP → |08 06|
  - Offset Option: Start inspection at byte 12 in the Ethernet frame
  - Depth Option: Inspect 2 bytes only
  - Threshold Mechanism: Define a limit for the number of matched ARP packets occurring within a 1-seconds interval

Suricata Rule for Mediaplayer POST Flooding Attack

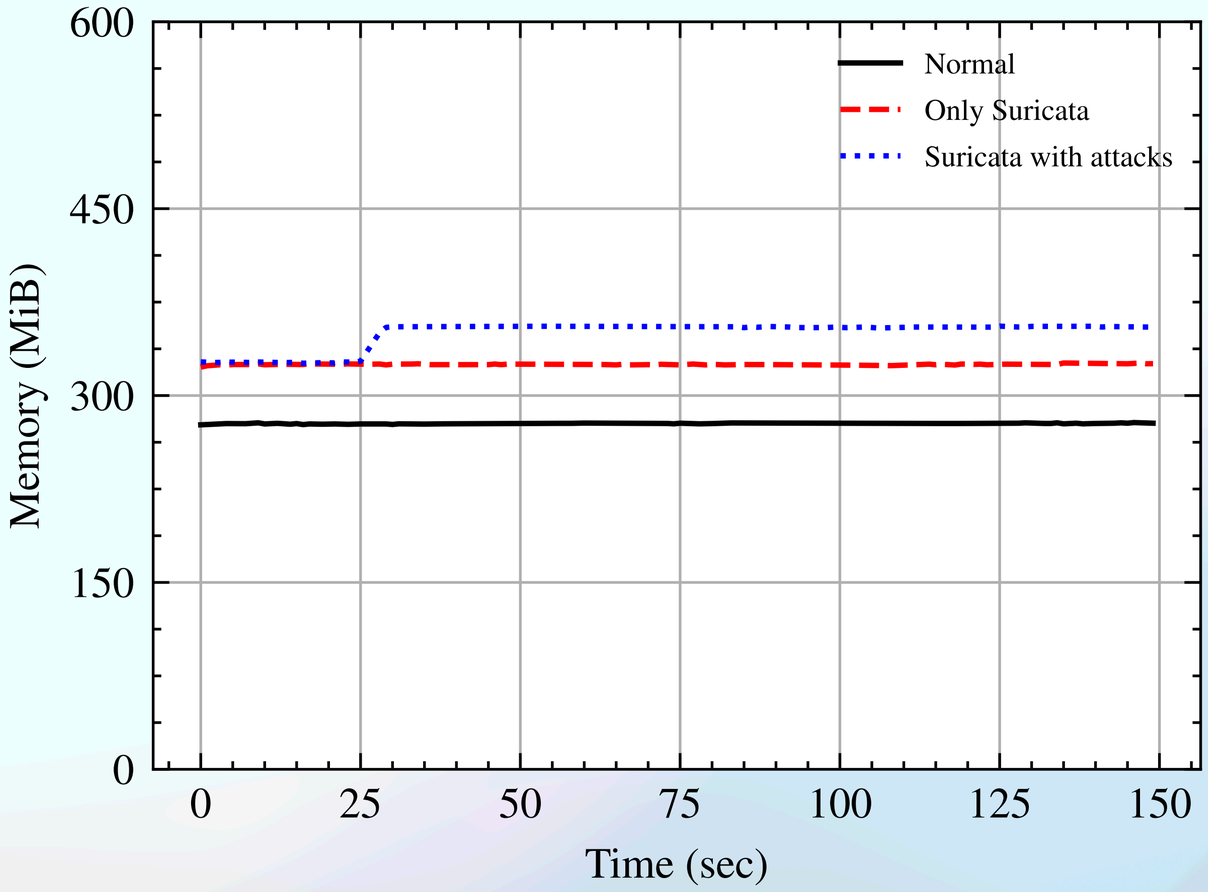
★ **Detection Metric: SYN Packet Volume**

- Normal Behavior: Characterized by standard network management traffic, such as IGMP for subnet management and SSDP for service discovery
- Attack Behavior: Indicated by a significant and abnormal surge in SYN packets, which is a key indicator of a SYN flood attack
- Detection Rule Logic
  - Filter: A flag (e.g., the 's' option) is used to specifically isolate and count packets with the SYN flag set
  - Threshold: A rate-limiting threshold defines the maximum number of SYN packets permitted per second before an alert is triggered

Result



Experiment Result: CPU Usage



Experiment Result: Memory Usage

Result

Attack scenarios	Attack interval (Seconds)	Alerts within the attack interval	Total number of alerts	Detection
Port scanning	1.70 - 8.78	18	18	Success
Phone dialing spoofing	2.06 - 5.18	200	200	Success
Navigation map pharming	6.38 - 55.25	36	36	Success
Multiple session DoS	6.54 - 7.70	6	6	Success

Summary of Detection Results for the Tested Attack Scenarios

Conclusion

Attack Scenario Identification in IVI Systems

- IVI systems are exposed to diverse security threats, including:
  - Location data leakage, navigation manipulation, abuse of communication features, DoS attacks, etc…
- Scope of impact extends beyond expectations:
  - Initially assumed to be limited to internal IVI interfaces
  - Confirmed ability to affect CAN bus and external devices via Bluetooth connectivity

Attack Classification and Multi-phase Attack Sequence Analysis

- Attacks classified into five classifications:
  - Reconnaissance, Exfiltration, Manipulation, Redirection, DoS(Denial-of-Service)
- Systematic mapping to MITRE ATT&CK framework enables structured analysis of TTPs
- Realistic multi-phase attack sequences defined targeting:
  - Navigation App → port scanning & location tracking & destination spoofing
  - Phone App → port scanning & phone data leakage & fraudulent dialing
  - Messaging App → port scanning & message data leakage & message hijacking & service disruption
- Emphasis on privacy violations and personal data exposure

Detection of IVI Attacks Using Suricate

- Suricata-based IDS successfully detects 4 major attack scenarios
  - Demonstrated precise, time-bounded detection capability
- Resource usage within acceptable limits for embedded environments:
  - CPU usage: up to 22%
  - Memory consumption: approx. 327 MiB
- Results indicate feasibility of integrating Suricate into in-vehicle systems for real-time intrusion detection

Future Work

- Detection mechanism for remaining attack scenarios
  - Current implementation successfully detects 4 out of 11 defined scenarios
  - Requires development of detection logic for the remaining 7 undetected scenarios

- Automated Suricata Rule Generation Framework
  - Manual rule creation is time-consuming and error-prone
  - Develop a rule generation platform that automatically translates attack signature and patterns into Suricate-compatible rules

- Automated Suricata Rule Generation Framework
  - To ensure generalizability, experiments must be replicated on alternative IVI system such as QNX, etc...

Q & A

Thank You.
감사합니다.