Challenge of VIN

2025. 10. 17.

순천향대학교 시스템보안연구실
LAB. OF INFORMATION SYSTEMS SECURITY ASSURANCE

Table of Contents

Challenge of VIN

I Introduction

□ VIN data extraction through CAN Bus communication analysis

○ Objective

— Participants can extract Vehicle Identification Number (VIN) by connecting to remote CAN Bus interface and communicating with ECU simulator.

○ Components

— Remote CAN interface connection info (IP, Port)

Ⅱ Problem Scenario and Step-by-Step Solution Path

□ Remote CAN Bus Connection

○ Participants connect to provided server

— Server IP and Port will be provided

-- Use netcat for connection

— Verify connection by monitoring CAN traffic

□ VIN Data Request and Extraction

○ Participants send VIN request using OBD-II protocol

— Send Service 09 PID 02 request: 7DF#020902

— Receive first frame with total data length

— Identify multi-frame response structure

○ Handle multi-frame communication

— Send Flow Control frame: 7DF#30000000000000

— Collect consecutive frames in sequence

— Assemble fragmented data packets correctly

○ Decode VIN data

— Convert hex bytes to ASCII characters

— Extract complete 17-character VIN string

Ⅲ Flag Conditions

□ FLAG Acquisition

○ The extracted VIN itself is the flag