Challenge of FOTA

2025. 10. 17.

순천향대학교 시스템보안연구실

LAB. OF INFORMATION SYSTEMS SECURITY ASSURANCE

Table of Contents

Challenge of FOTA

I Introduction

□ Firmware extraction and analysis through FOTA packet capture files

○ Objective

— Participants can extract and analyze firmware by examining FOTA technology packets commonly used in actual vehicles.

○ Components

— pcap file

Ⅱ Problem Scenario and Step-by-Step Solution Path

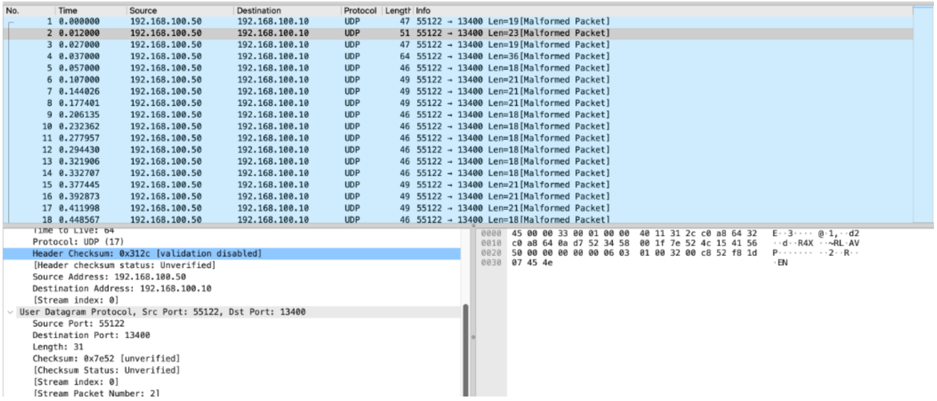
□ Packet Capture File Analysis

○ Participants analyze the provided packet capture image

— Specific SOF and EOF can be found in UDP communication

-- The structure of packets can be analyzed by referring to the protocol guidelines

— It can be confirmed that sequence numbers are mixed



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.100.50	192.168.100.10	UDP	47	55122 → 13400 Len=19[Malformed Packet]
2	0.012000	192.168.100.50	192.168.100.10	UDP	51	55122 → 13400 Len=23[Malformed Packet]
3	0.027000	192.168.100.50	192.168.100.10	UDP	47	55122 → 13400 Len=19[Malformed Packet]
4	0.037000	192.168.100.50	192.168.100.10	UDP	64	55122 → 13400 Len=36[Malformed Packet]
5	0.057000	192.168.100.50	192.168.100.10	UDP	46	55122 → 13400 Len=18[Malformed Packet]
6	0.107000	192.168.100.50	192.168.100.10	UDP	49	55122 → 13400 Len=21[Malformed Packet]
7	0.144026	192.168.100.50	192.168.100.10	UDP	49	55122 → 13400 Len=21[Malformed Packet]
8	0.177401	192.168.100.50	192.168.100.10	UDP	49	55122 → 13400 Len=21[Malformed Packet]
9	0.206135	192.168.100.50	192.168.100.10	UDP	46	55122 → 13400 Len=18[Malformed Packet]
10	0.232362	192.168.100.50	192.168.100.10	UDP	46	55122 → 13400 Len=18[Malformed Packet]
11	0.277957	192.168.100.50	192.168.100.10	UDP	46	55122 → 13400 Len=18[Malformed Packet]
12	0.294430	192.168.100.50	192.168.100.10	UDP	46	55122 → 13400 Len=18[Malformed Packet]
13	0.321906	192.168.100.50	192.168.100.10	UDP	46	55122 → 13400 Len=18[Malformed Packet]
14	0.332707	192.168.100.50	192.168.100.10	UDP	46	55122 → 13400 Len=18[Malformed Packet]
15	0.377445	192.168.100.50	192.168.100.10	UDP	49	55122 → 13400 Len=21[Malformed Packet]
16	0.392873	192.168.100.50	192.168.100.10	UDP	49	55122 → 13400 Len=21[Malformed Packet]
17	0.411998	192.168.100.50	192.168.100.10	UDP	49	55122 → 13400 Len=21[Malformed Packet]
18	0.448567	192.168.100.50	192.168.100.10	UDP	46	55122 → 13400 Len=18[Malformed Packet]

```
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x312c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.100.50
    Destination Address: 192.168.100.10
    [Stream index: 0]
  User Datagram Protocol, Src Port: 55122, Dst Port: 13400
    Source Port: 55122
    Destination Port: 13400
    Length: 31
    Checksum: 0x7e52 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Stream Packet Number: 2]
```

```
0000  45 00 00 33 00 01 00 00  40 11 31 2c c0 a8 64 32   E··3···· @·1,··d2
0010  c0 a8 64 0a d7 52 34 58  00 1f 7e 52 4c 15 41 56   ··d··R4X ··~RL·AV
0020  50 00 00 00 00 00 06 03  01 00 32 00 c8 52 f8 1d   P······· ··2··R··
0030  07 45 4e                                           ·EN
```

□ Firmware Extraction

○ Participants write extraction code using Python

○ Convert the extracted firmware into a file system using tools such as binwalk

Ⅲ Flag Conditions

□ FLAG Acquisition

○ Obtain the flag from a secret file inside the firmware