Security Analysis of an In-Vehicle-Infotainment and App Platform

Sahar Mazloom, Mohammad Rezaeirad, Aaron Hunter
Security Lab, George Mason University

and Damon McCoy
New York University
Modern Cars: PCs on wheels

• ECU (Electronic Control Unit)
  – Monitor and Control different subsystems of a car
    • From Engine Control and Braking System
e    to Driver Assistance & Multimedia Systems

• CAN (Controller Area Network)
  – Handles ECUs communications
  – Message-based protocol
  – Broadcast Nature

Image source: munic.io
Modern Cars: PCs on wheels

• ECU (Electronic Control Unit)
  – Monitor and Control different subsystems of a car
    • From Engine Control and Braking System
      to Driver Assistance & Multimedia Systems

• CAN (Controller Area Network)
  – Handles ECUs communications
  – Message-based protocol
  – Broadcast Nature
  – Previous **Attacks** against it
    – UCSD & UW
    – Miller & Valasek
Head Units vs User Demands
Connected Cars

There is no doubt that cars are getting connected to infrastructure, other cars, machines, cloud, eCall.

Consumers want to be connected everywhere, being always online.

“People feel disconnected from friends while driving.”

Smartphone connectivity solutions are standardized except in cars.
Governed by Car Connectivity Consortium (CCC) 2011
Cars Lineup

Hyundai
Kia
Toyota
Buick
Chevrolet
Honda
DS Automobiles
Mazda
GM
Mercedes-Benz
Volkswagen
Peugeot
Subaru
Volkswagen Group
Citroën
Seat
Smart
Byd
Smartphones Lineup

- Samsung
- Sony
- HTC: quietly brilliant
- LG: Life's Good
- Windows Phone
- BlackBerry
- Huawei
Can someone control your car by infecting your smartphone?
Starting Our Security Assessment

MirrorLink was disabled!

Tuners know how to enable it!!
Enabling MirrorLink on IVI

Credit goes to Car tuners and garage workers

Activated!
MirrorLink Components

IVI (Client)

Smartphone (Server)
RE Procedure: Communication Traffic Analysis
Protocol Stack: VNC protocol

VNC: Virtual Network Computing
Protocol Stack:
UPnP

UPnP: Universal Plug and Play
### MirrorLink Configuration Files (XML)

**Figure 4.2.3: GET and POST request messages sent by IVI and replies by the smartphone**

<table>
<thead>
<tr>
<th>GET/POST requests sent by IVI and replied by Smartphone</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET &amp; POST requests sent by IVI and replied by Smartphone</td>
</tr>
</tbody>
</table>
Lab Setup

Hardware
RE
Entering Development Mode
Static Binary Analysis

- Binary Files responsible for MirrorLink in IVI Firmware
  - TMSControlPoint.DLL
  - AppTm.EXE

- Protection Mechanisms
  - /GS
  - ASLR
  - DEP
  - SafeSEH
  - Heap Guard

<table>
<thead>
<tr>
<th>Binary Name</th>
<th>ASLR</th>
<th>Stack Cookies</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppLink.exe*</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>AppMain.exe°</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>ML_CERTIFICATION.dll*</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>CmnDll.dll®</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>MgrMcm.exe°</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>MgrSys.exe°</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>MgrVid.exe°</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>AppTM.exe*</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>TMScontrolPoint.dll*</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
</tbody>
</table>
<xml version="1.0" encoding="utf-8"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
          s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
      <s:Body>
        <u:GetApplicationListResponse xmlns:u="urn:schemas-upnp-org:service:TmApplicationServer:1">
          <appList>
            <appid>Mo</appid>
            <name>SaharAAAAAAA</name>
            <icon><mime>image/png</mime>
                  <width>300</width>
                  <height>300</height>
                  <depth>32</depth>
                  <url>/car.png</url></icon>
            <providerName>Samsung Electronics</providerName>
          </appList>
        </u:GetApplicationListResponse>
      </s:Body>
    </s:Envelope>
<?xml version="1.0" encoding="utf-8"?>
<Envelope xmlns:ns1="http://schemas.xmlsoap.org/soap/envelope/"
         xmlns:ns2="http://schemas.xmlsoap.org/soap/encoding/>
   <Body>
     ...<u:GetApplicationListResponse xmlns:urn="urn:schemas-upnp-org:service:TmApplicationServer:1">
       <appList>
         <appID>Mo</appID>
         <name>SaharAAAAAAAAAAAAAAAAAAAABBBBCCCCDDDEEEEFFFFGGGHIJKLMNOPQRSTUVWXYZ</name>
         <icon>&lt;/icon&gt;
         <mimetype>image/png</mimetype>
         <width>300</width>
         <height>300</height>
         <depth>32</depth>
         <url>/car.png</url>
       </appList>
     ...
UART Debug Messages

Exception 'Access Violation' (2): Thread-Id=061300a6(pth=853039c8), Proc-Id=052e001e(pprc=87b8f540) 'AppTm.exe', VM-active=052e001e(pprc=87b8f540) 'AppTm.exe'
PC=421d15d8c(tmscontrolpoint.dll+0x000115dc) RA=421d168c(tmscontrolpoint.dll+0x0001168c)
SP=0020f620, BVA=4848484c

ShowErr is running (ExcpCode : c0000005 / ExcpAddr : 421d15dc)
[ShowErr] MgrTsk (0x70021b40)!!!!

Exception 'Alignment Error' (4): Thread-Id=06ea0006(pth=85294978), Proc-Id=05940026(pprc=87b59440) 'AppTm.exe'
VM-active=05940026(pprc=87b59440) 'AppTm.exe'
PC=421c41c8(tmscontrolpoint.dll+0x000041c8) RA=421c41d0(tmscontrolpoint.dll+0x000041d0) SP=001ff5e0, BVA=00000000
ShowErr is running (ExcpCode : 80000002 / ExcpAddr : 421c41c8)
[ShowErr] MgrTsk (0x70021b40)!!!!

OEMInterruptDisable:: DDMA:maskc, inten:ff
[DRVMGR] BT reset
OEMInterruptDisable:: DDMA:maskc, inten:ff
Static Analysis

Unsafe libc functions are found!
Dynamic Debugging
Buffer Overflow
From Vulnerability to Exploit

Goal: Overwriting Function Pointer

issue: Taking care of Data Pointers (Overwriting with valid addresses)
Exploit Chain

✓ Overflow Buffer on Heap
✓ Overwrite Function Pointer

```
#include <stdio.h>

int main()
{
    char buffer[100];
    // Store exploit code in buffer
    // Call function to trigger exploit
    return 0;
}
```
Exploit Chain

- Same CAN controller used in Jeep Attack
- Miller & Valasek modified list of CAN IDs by updating that part of the Micom firmware

- An attacker can send any arbitrary CAN packet
Responsible Disclosure plan

• Initial private disclosure (more than 11 month ago), delayed publication, and left out critical details.

• No name/No shame/No details

• Can affect other manufacturers

• Additional time to patch the vulnerabilities
What this ALL mean

• Bring to light the current insecurities of these IVI and app platforms before they become widely deployed

• Design & Implement with security in mind
  • Before integrating automobiles with 3rd party App ecosystem
my apps

Thank you from George Mason!

Welcome to ask questions

edit message alert