The Future Is Here - Modern Attack Surface On Automotive

Lior Yaari & Yonatan Migdal

30/08/2019
Yonatan

Lior

Casual

Hobby

Techy

Cool

7 Years In Cyber Security

Sec-Dev Consultant

Bug Bounty-er

Robotics Geek

CS Teacher

Moving To Italy

Studying German

Acroyogist

Born In Jerusalem

CS Teacher

Moving To Italy

Studying German

Acroyogist
End to End Security Testing

Breaking through the cloud or factory

Bypassing ECU protections

Vehicle Security Research

Building Security Products

Automotive SOC Prevention Concepts

IDS

IPS
Disclaimer

As part of our job with CYMOTIVE we are working closely with several automotive companies and because of that many of our findings are under NDA.

We will not include ANY customer names and real issues which can cause any harm and focus more on the tech side.

* All photos in this presentation are from open sources found on the internet
Progress Bar

- Who We Are
- Automotive Past & Future
- Connected Technologies
- Centralized Management
Automotive Main Trends

- NFC
- Wifi
- Bluetooth
- PLC
- V2X
- GPS
- LiDAR
- SLAM
- Sonar
- Thermo
Who talks to my car?

Year 2005~
Who talks to my car?

Year 2015~
Who talks to my car?

Year 2025~
What does it imply?
Changes

- CAN Bus
  - Mechanical Engineer

- Ethernet
  - Software Developer
New Demands

Vehicle Clouds

Growing IT Department

Tons of Infosec Jobs
VEHICLES

HACKERS

HACKERS
Some Terminology

Original Equipment Manufacturer (OEM)
Some Terminology

Electronic Control Unit (ECU)
Some Terminology

Infotainment
(Information + Entertainment)
Progress Bar

• Who We Are
• Automotive Past & Future
• Connected Technologies
• Centralized Management

LET THE FUN BEGIN
The new fashion in vehicle IoT are “Aftermarket Solutions”

Which are also the solution for hackers
Aftermarket Solutions

Chainway TSP

Vinli OBD-II

Samsung

Engie

Viper Smart Start

Drone Mobile

MYCAR

Engie

1-year service plan included!
Hacking the: Server, Phone, Dongle

->

Hacking the car
Keyless Entry $\Rightarrow$ Car Sharing
By Continental
https://www.youtube.com/watch?v=vdnrr5i4naE
A REMOTE-START APP EXPOSED THOUSANDS OF CARS TO HACKERS

More Than 100 High-End Cars Were Stolen Using An App In A Possible Chicago Crime Spree

All 100 vehicles, including at least 50 Mercedes-Benz cars, that were reported missing are being recovered, the company said on Thursday.

Stephanie K. Baer
BuzzFeed News Reporter

Last updated on April 18, 2019, at 10:48 a.m. ET
Posted on April 17, 2019, at 9:34 p.m. ET
The Bluetooth Problem

Infotainment, Dongles, Keys are all Bluetooth connected

- Hell2CAP (Cymotive)
  - CVE-2018-20378
- KNOB (SUTD)
  - CVE-2019-9506
- BleedingBit (Armis)
  - CVE-2018-16986
  - CVE-2018-7080
Hell2CAP

Found by Barak Caspi at Cymotive

State machine bug in BlueSDK L2CAP (~100 Million Devices)
L2CAP Channel Multiplexing

PSM – “Protocol ID”

L2CAP_Connect(PSM=0x1)
L2CAP Channel Multiplexing

PSM – “Protocol ID”
DCID – channel identifier

L2CAP_Connect(PSM=0x1)
L2CAP_ConnectResp(DCID=0x41)
L2CAP Channel Multiplexing

PSM – “Protocol ID”
DCID – channel identifier

L2CAP_Connect(PSM=0x1)
L2CAP_ConnectResp(DCID=0x41)
L2CAP_ConfReq(DCID=0x41, ...)

CYMOTIVE TECHNOLOGIES
L2CAP Configuration
Can config: MTU, Timeout and more

Minimal Bluetooth MTU is 48

local device can receive, in this channel, an MTU larger than the minimum required. All L2CAP implementations shall support a minimum MTU of 48 octets, however some protocols and profiles explicitly require support for a

- Bluetooth Specification Version 3.0 + HS [Vol 3]
L2CAP Configuration

```c
if ( config_option[1] == ConfigOption_MTU )
{
    in_mtu = LEtoHost16(data_iter + 2);
    channel->MTU = in_mtu;
    if ( channel->ptProtocol->minimum_protocolMTU > in_mtu )
    {
        l2cap_set_channel_as_invalid(channel);
    }
}
```

- Save MTU
- Check Size
- Set Invalid
- On Fail
L2CAP Configuration

Connect

Channel 0x41
Valid – Yes
MTU – 0x500
L2CAP Configuration

- Connect
- L2CAP_ConfReq(DCID=0x41, MTU=0x200)
- L2CAP_ConfResp(DCID=0x41, SUCCESS)

- Channel 0x41
  - Valid – Yes
  - MTU – 0x200
L2CAP Configuration

L2CAP_ConfReq(DCID=0x41, MTU=0x10)

L2CAP_ConfResp(DCID=0x41, INVALID)

Connect

Channel 0x41
Valid – No
MTU – 0x10

L2CAP Configuration
Hell2CAP

Red flag – Values is stored (4) than checked (5)
Can we restore channel to be valid?

```c
if ( config_option[1] == ConfigOption_MTU ) {
    in_mtu = LEtoHost16(data_iter + 2);
    channel->MTU = in_mtu;
    if ( channel->ptProtocol->minimum_protocolMTU > in_mtu ) {
        l2cap_set_channel_as_invalid(channel);
    }
}
```
Hell2CAP

Red flag – Values is stored (4) than checked (5)
Can we restore channel to be valid?

ConfigRequest (MTU = 20) ➔ Channel Invalid, ch.MTU = 20 ➔ ConfigRequest (FlushTimeout = 0x1337) ➔ Channel Valid ch.MTU = 20
Hell2CAP

On upper layer – SDP there is fragmentation code

```c
MTU = L2CAP_GetTxMtu(_sdpInfo->CID);
availableSizeForFragment = (MTU - 9) & 0xFFFF;
...
SdpStoreAttribData(_sdpInfo, _txPkt, _txPkt->bufferPtr, availableSizeForFragment);
```

MTU from L2CAP, we control it
Hell2CAP

On upper layer – SDP there is fragmentation code

MTU = 48 -> availableSizeForFragment = 48 – 9 = 39
MTU = 8 -> availableSizeForFragment = 8 – 9 = 0xFFFF

Integer underflow
Hell2CAP

- Set Low MTU
- Integer Underflow
- Buffer Overflow
- Profit
The problem with Bluetooth is that it is not the only problem.
V2X – Vehicle to X
This increases existing road capacity, enhances mobility and reduces emissions.
V2X payload is ASN.1 based
A fake V2X module could:

- Create False Traffic
- Force Emergency Breaks
- Generate False Alarms
Charging Evolution
Charging PLC

EVSE – Electric Vehicle Supply Equipment
PEV – Plug-in Electric Vehicle
Charging PLC

PLC – Power Line Communication
Charging Protocol Stack

- Wired / Ethernet
- IPv6
- TCP
- UDP
- SDP
- HPGP
- Vendor Specific
- SLAC
- XML-EXI
- V2GTP
- TLS
- IPv6
- Wired / Ethernet
XML Parsers Vulns

Header Edge Cases

Vendor Specific

SLAC
UDP
TCP
HPGP
IPv6
Wired / Ethernet

XML-EXI
V2GTP
SDP
TLS
TCP
IPv6
Wired / Ethernet
VxWorks TCP/IP Stack CVEs by Armis Labs (19.7.2019):

**IP RCE:** CVE-2019-12256

EVSE! Use Buffer Overflow!
Hackers Benefits

Charge your credit card and not your car
Hack other ECUs from PEV
Progress Bar

- Who We Are
- Automotive Past & Future
- Connected Technologies
- Centralized Management
Hackers Benefits

Vehicle Clouds

EVSEs are all cloud connected
The Vehicle Cloud

The Magical Place Where Everything Is Possible
(For a Hacker)
The Vehicle Cloud

Normal Stuff
- Private Information
- Credit Cards
- OEM Secrets

Juicy Stuff
- GPS Coordinates
- Remote Unlock
- OTA Updates
Futuristic Stuff
Centralized Control for Shared Transportation

Next-Gen Police

The cloud is the limit…
OTA – Over The Air

Most modern cars receive software updates with 4G connection to the OEM servers
The Vehicle Cloud

Update

Update

Update

Update
The Vehicle Cloud
STOP! Pay 5000$ to unlock this car
The bright side

OEMs invest immense efforts in cyber security

Connected autonomous would be really great
Risks

Everything Is Connected

New Attack Vectors – BT, Wifi, NFC, V2X, PLC

Opportunities

Less Accidents

Life Changing Technologies
Ask Us Anything
Lior.yaari@cymotive.com
Lior@imperium-sec.com

Yonatan.migdal@cymotive.com