THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

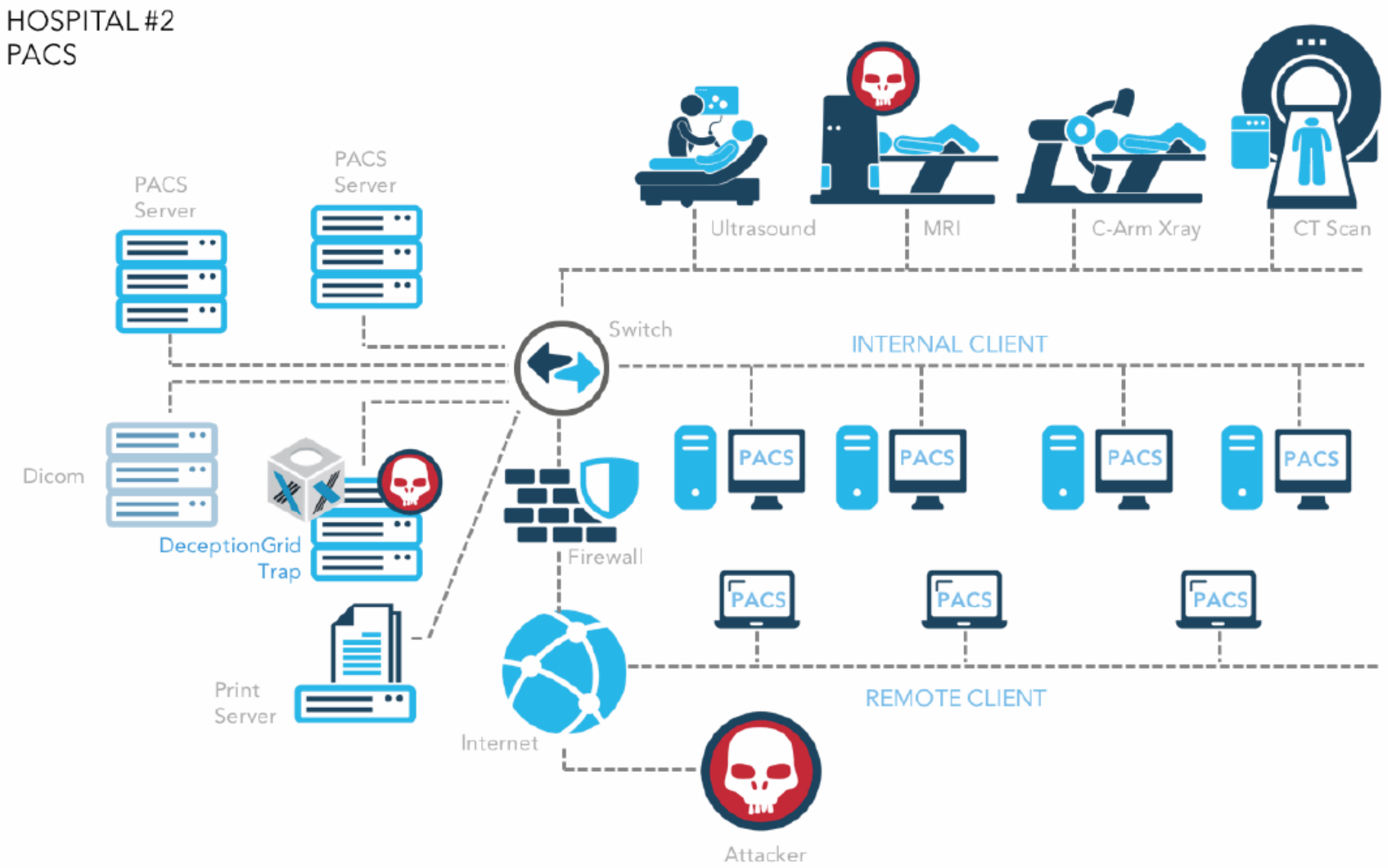
Lessons Learned From A Vulnerable IoT Application

Daniel Xiapu Luo

Department of Computing

The Hong Kong Polytechnic University

US hospitals hacked with ancient exploits



http://deceive.trapx.com/rs/929-JEW-675/images/AOA_Report_TrapX_MEDJACK.2.pdf[2]

The company says the modern security systems in place at the hospitals did not eradicate the old malware using vulnerabilities such as MS08-067 which was dangerous only to Windows XP systems.

Internet-connected Hello Barbie doll can be hacked

The iconic toy becomes a connected device, and promptly gets pegged for security issues.

2 COMMENTS

Jared Newman | *@onejarednewman* Dec 7, 2015 9:17 AM
PCWorld

In news that should surprise no one, connecting a toy to the Internet invites the risk of hacking.

So it went with Hello Barbie, which lets children converse with the doll over a cloud server connection. As reported by the *Wall Street Journal*, BlueBox Security and independent researcher Andrew Hay uncovered several vulnerabilities in the toy, the worst of which could allow an attacker to intercept a child's communications.

The good news is that ToyTalk, which partnered with Mattel on Hello Barbie, has been

VTech hack exposes ID theft risk in connecting kids to Internet

VTech's products are seen on display at a toy store in Hong Kong, China November 30, 2015. REUTERS/Tyrone Siu 1/2

By **Jim Finkle** and **Jeremy Wagstaff** | BOSTON/SINGAPORE

Parents who gave their child a Kidizoom smartwatch or a VTech InnoTab tablet may have exposed them to identity theft after Hong Kong-based VTech said hackers stole the personal information of more than 6 million children.

Watch out, new parents—internet-connected

Welcome Manufacturers Countries Places Cities Timezones New online cameras FAQ Contacts

IP cameras: Hong Kong

http://www.insecam.org/en/

« 1 2 3 4 5 »

atch Streamer camera in Hong Kong,Hong Kong

Watch PanasonicHD camera in Hong Kong,Hong Kong

Watch PanasonicHD camera in Hong Kong,Hong Kong

monitor to play the Police's "Every Breath You Take," followed by "sexual noises."

HP LaserJet Pro Printers remotely exploitable to gain unauthorized access to Wi-Fi and Printer Data

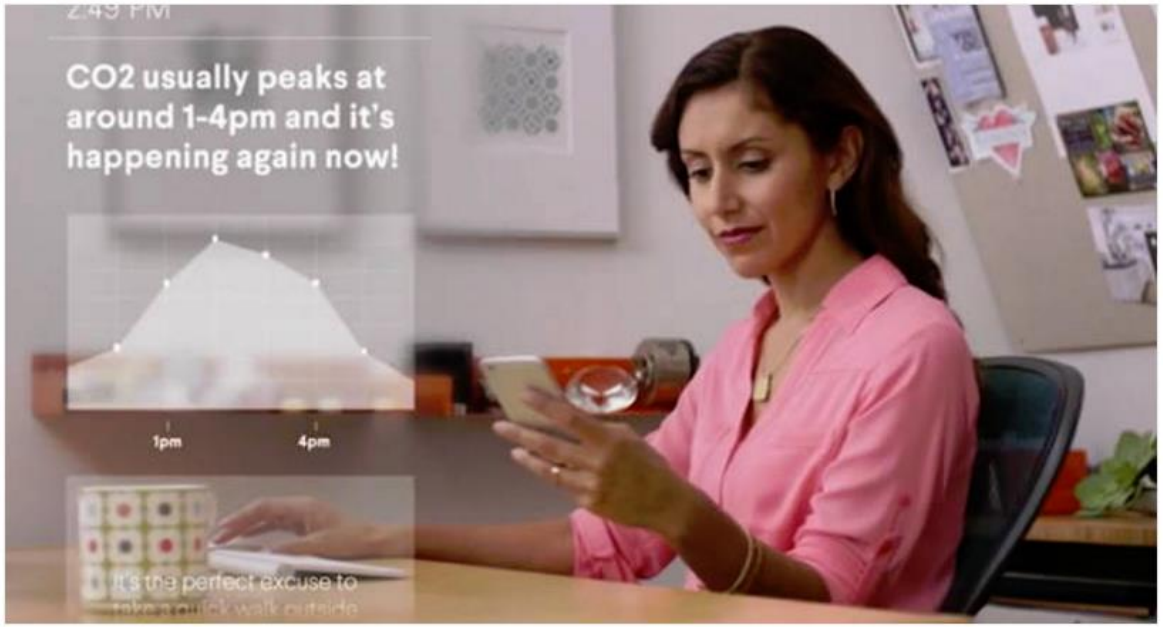
Tuesday, August 06, 2013 Mohit Kumar

G+1 73 Like 358 Share 558 Tweet 287 Share 18 share 6013

Do you own an HP printer? If so, it may be vulnerable to Hackers. Multiple HP LaserJet Pro Printers are printer vulnerable to hackers according to a new advisory posted by the vendor, dubbed as CVE-2013-4807 (SSRT101181).

Samsung smart fridge leaves Gmail logins open to attack

Failures in exploit discovery process are cold comfort for IoT fridge owners



24 Aug 2015 at 09:03, John Leyden 409

Update Security researchers have discovered a potential way to steal users' Gmail credentials from a Samsung smart fridge.

Pen Test Partners discovered the MiTM (man-in-the-middle) vulnerability that facilitated the exploit during an IoT hacking challenge at the recent DEF CON hacking conference.

ANDY GREEN

HACKERS CUT A CORVETTE'S BRAKES VIA A COMMON CAR GADGET

ANDY GREENBERG SECURITY 08.11.15 7:00 AM

Security researchers Karl Koscher and Ian Foster. RYAN YOUNG FOR WIRED

: Via Flickr

CAR HACKING DEMOS like last month's over-the-internet hijacking of a Jeep have shown it's possible for digital attackers to cross the gap between a car's cellular-connected infotainment system and its steering and brakes. But a new piece of research suggests there may be an even easier way for hackers to wirelessly access those critical driving

CONTENT

- Telematics and OBD-II
- Attack Surface of Telematics Systems
- A Vulnerable Telematics Device
- Exploit and Attacks
- Securing the Device
- Summary

Telematics

1 They fit a clever lit
your car

3 View feedback on h
driving

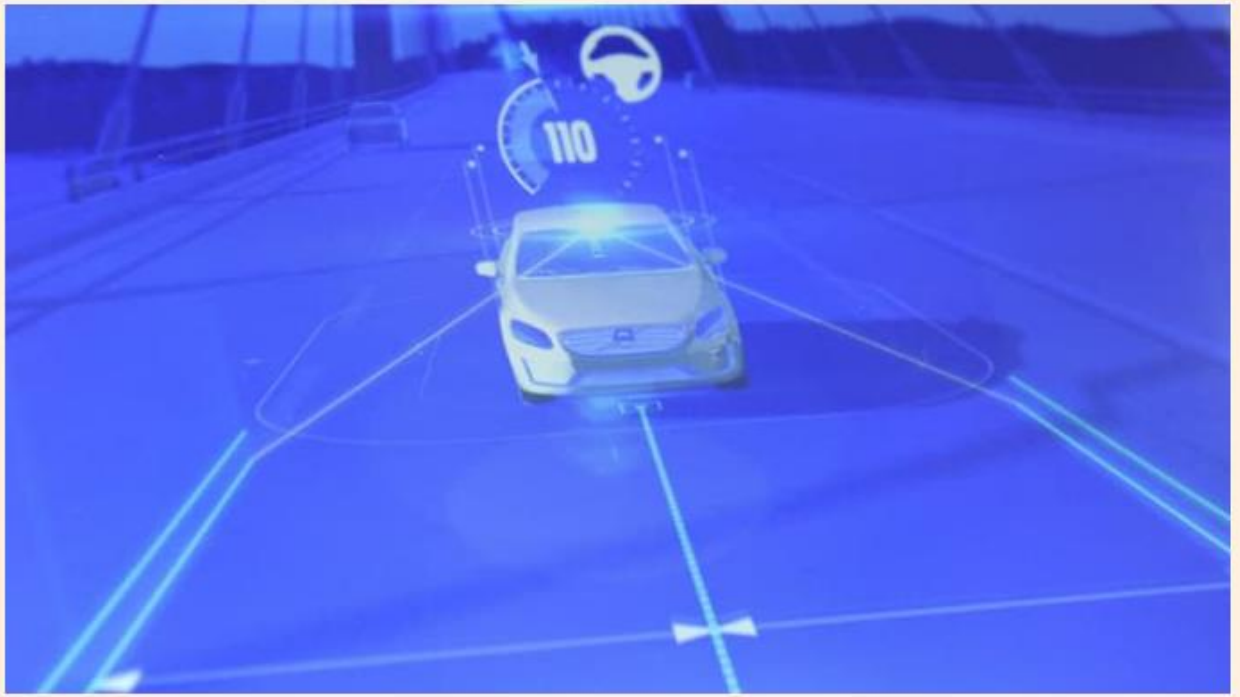
https://www.confused.

The glo
million
being d
on road
of telen

$140,100
ket is
blic safety
s. The use
culate

Telematics is revolutionising fleet management

Drivers are reconciling themselves to in-vehicle measurement technology



© Getty

3 Save

APRIL 18, 2016 by: John Griffiths

Since its introduction 15 years ago, telematics has largely been regarded as a tool for recording where vehicles are and how long their journeys have taken. But as its technology becomes more sophisticated and fears of intrusive spying on drivers recede, telematics is now a vital part of fleet management.

¥399.00 銷量108

元征golox車聯網盒子golo4汽車OBD2行車電腦

golo科技8 廣東 深圳

¥688.00 銷量35

駕圖車聯網GPS定位器微型汽車跟蹤器OBD盒子

成都華歌科技 四川 成都

¥699.00 銷量1

元征golo6 移動Wifi OBD汽車檢測 GPS定位

[illegible] 廣東 深圳

¥157.00 銷量32

圖吧汽車衛士OBD行車電腦汽車檢測儀

golo專攤 廣東 深圳

¥99.00 銷量918

圖吧汽車衛士obd2藍牙行車電腦車載智能盒子故障診斷儀汽車

圖吧導航旗艦店 北京

¥59.00 銷量271

圖吧汽車衛士OBD行車電腦智能盒子 obd2藍牙汽車故障檢測儀

圖吧導航旗艦店 北京

¥218.00 銷量285

優駕車載智能盒子高級版OBD行車電腦汽車檢測儀藍牙HUD抬頭

優駕旗艦店 廣東 廣州

¥88.00 銷量26

車掙 樂乘盒子OBD2GPS 衛星定位車輛故障診斷行車記錄儀遠程

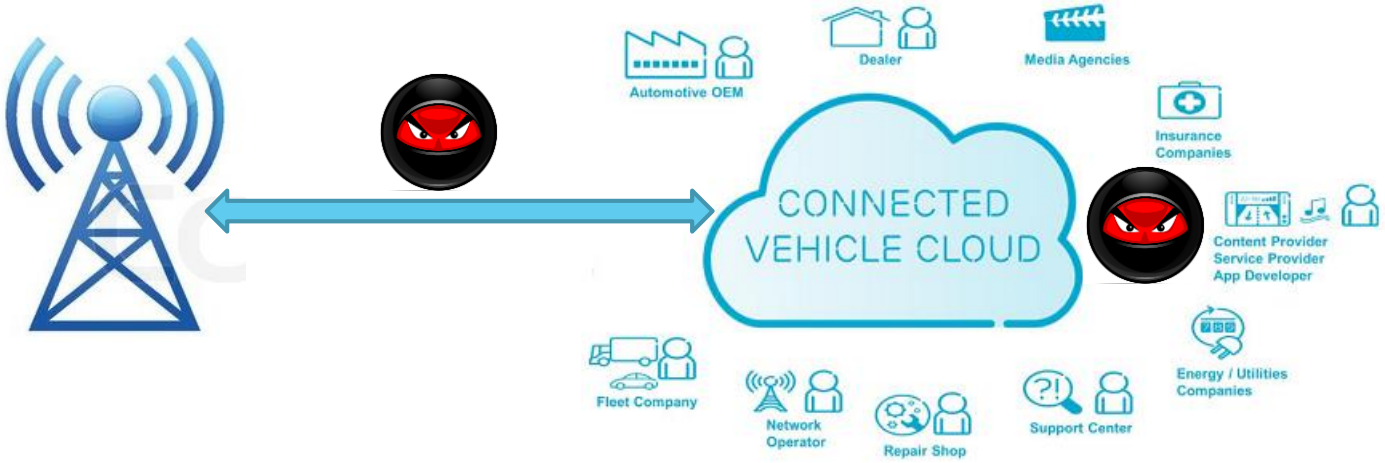
雅琴天下電子商務有限公司

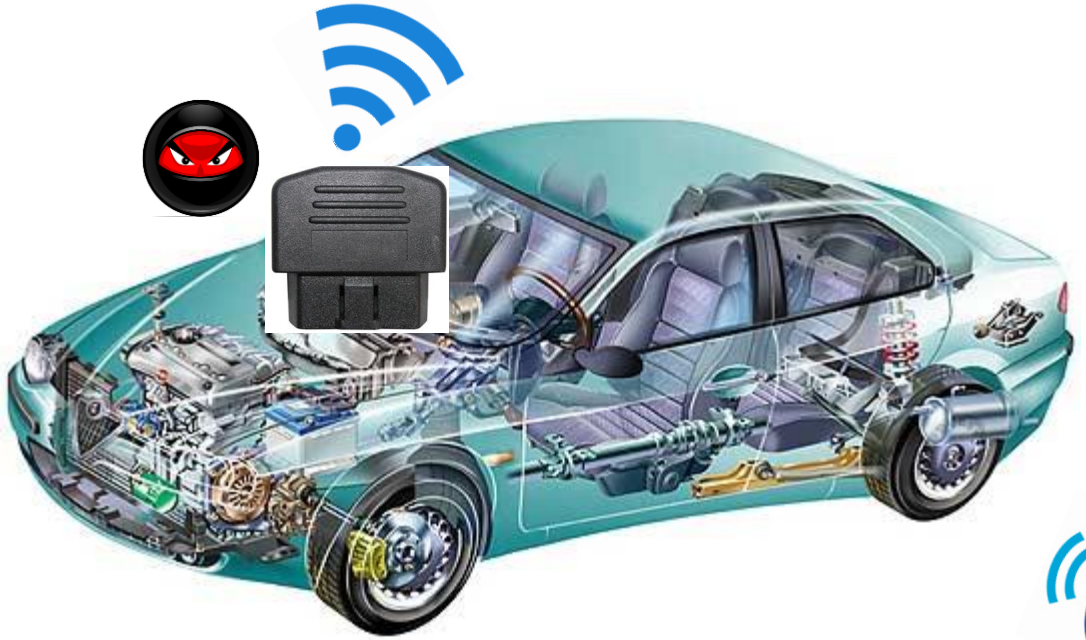
OBD-II

- On-Board Diagnostic
  - Perform emissions related diagnostics;
  - Collect information from ECUs;
  - Set ECU parameters;
  - Monitor engine and vehicle and even driver behaviors;
  - …

CONTENT

- Telematics and OBD-II
- Attack Surface of Telematics Systems
- A Vulnerable Telematics Device
- Exploit and Attacks
- Securing the Device
- Summary


Automotive OEM
Dealer
Media Agencies
Insurance Companies
CONNECTED VEHICLE CLOUD
Content Provider
Service Provider
App Developer
Energy / Utilities Companies
Fleet Company
Network Operator
Repair Shop
Support Center




Clever house

App – OWASP Mobile Top 10

M1 - Improper Platform Usage	M2 - Insecure Data Storage	M3 - Insecure Communication	M4 - Insecure Authentication
M5 - Insufficient Cryptography	M6 - Insecure Authorization	M7 - Client Code Quality	M8 - Code Tampering
	M9 – Reverse Engineering	M10 – Extraneous Functionality	

https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

Web Services – OWASP Web Top 10

- A1 - Injection
- A2 – Broken Authentication and Session Management
- A3 – Cross-Site Scripting (XSS)
- A4 – Insecure Direct Object References
- A5 – Security Misconfiguration
- A6 – Sensitive Data Exposure
- A7 – Missing Function Level Access Control
- A8 – Cross-Site Request Forgery (CSRF)
- A9 – Using Components with Known Vulnerabilities
- A10 – Unvalidated Redirects and Forwards

https://www.owasp.org/index.php/Top_10_2013-Table_of_Contents

Devices

- Insufficient Authentication/Authorization
- Lack of Transport Encryption
- Insecure Mobile Interface
- Insufficient Security Configurability
- Insecure Software/Firmware
- Poor Physical Security
- …

https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf

CONTENT

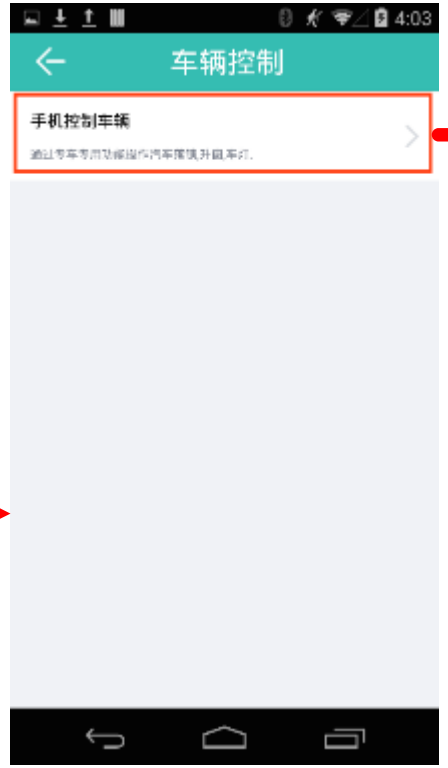
- Telematics and OBD-II
- Attack Surface of Telematics Systems
- A Vulnerable Telematics Device
- Exploit and Attacks
- Securing the Device
- Summary

Disclaimer

- For the vulnerable telematics device, we have informed the corresponding company about the vulnerabilities and how to patch them with the help of HKCERT.

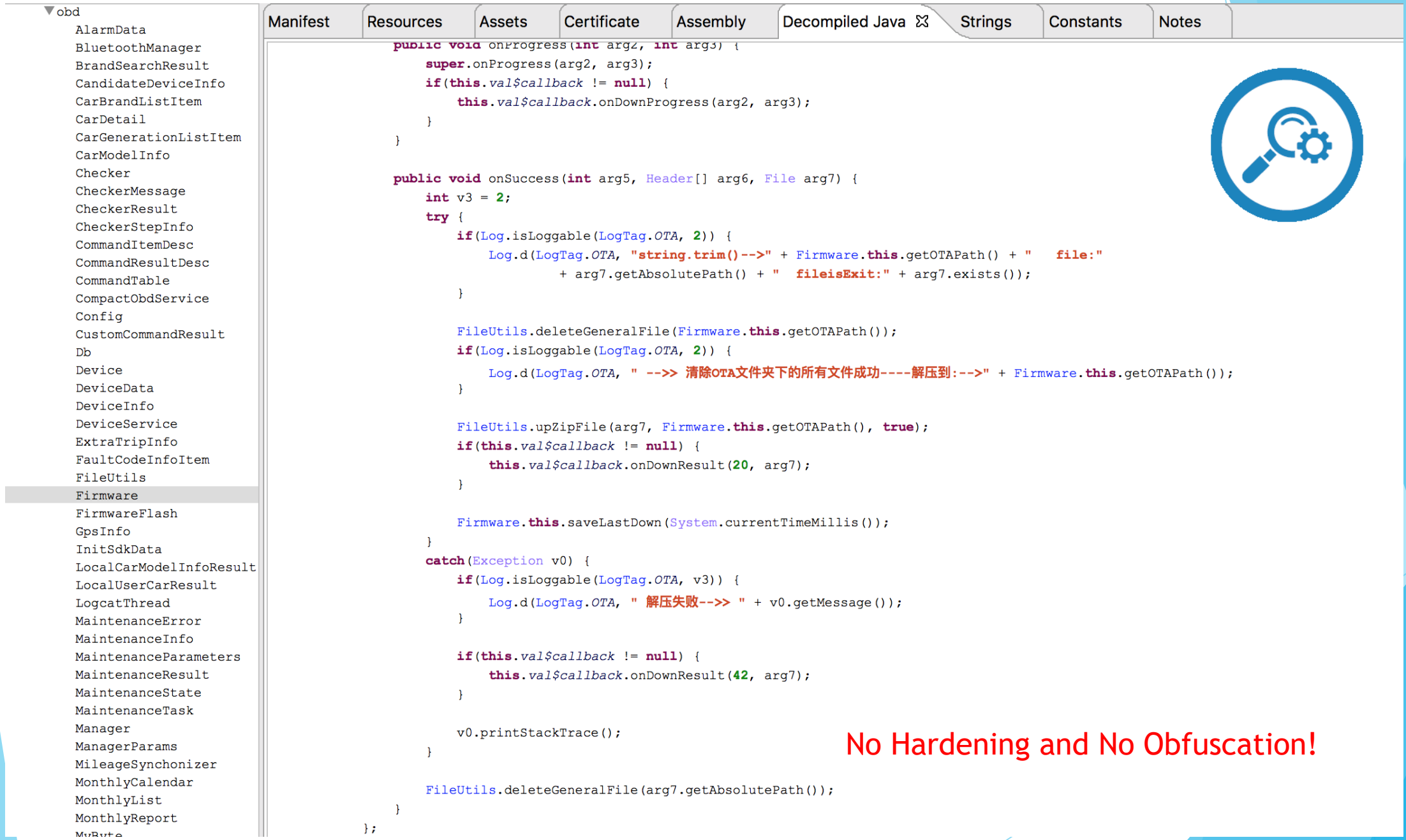
Mobile App


3:44
大众 迈腾
1.8TSI手动技术型 2007款
行程已被手动停止
重新连接
行程分析
爱车体检
爱车保养
胎压监测
燃油检测
车辆控制

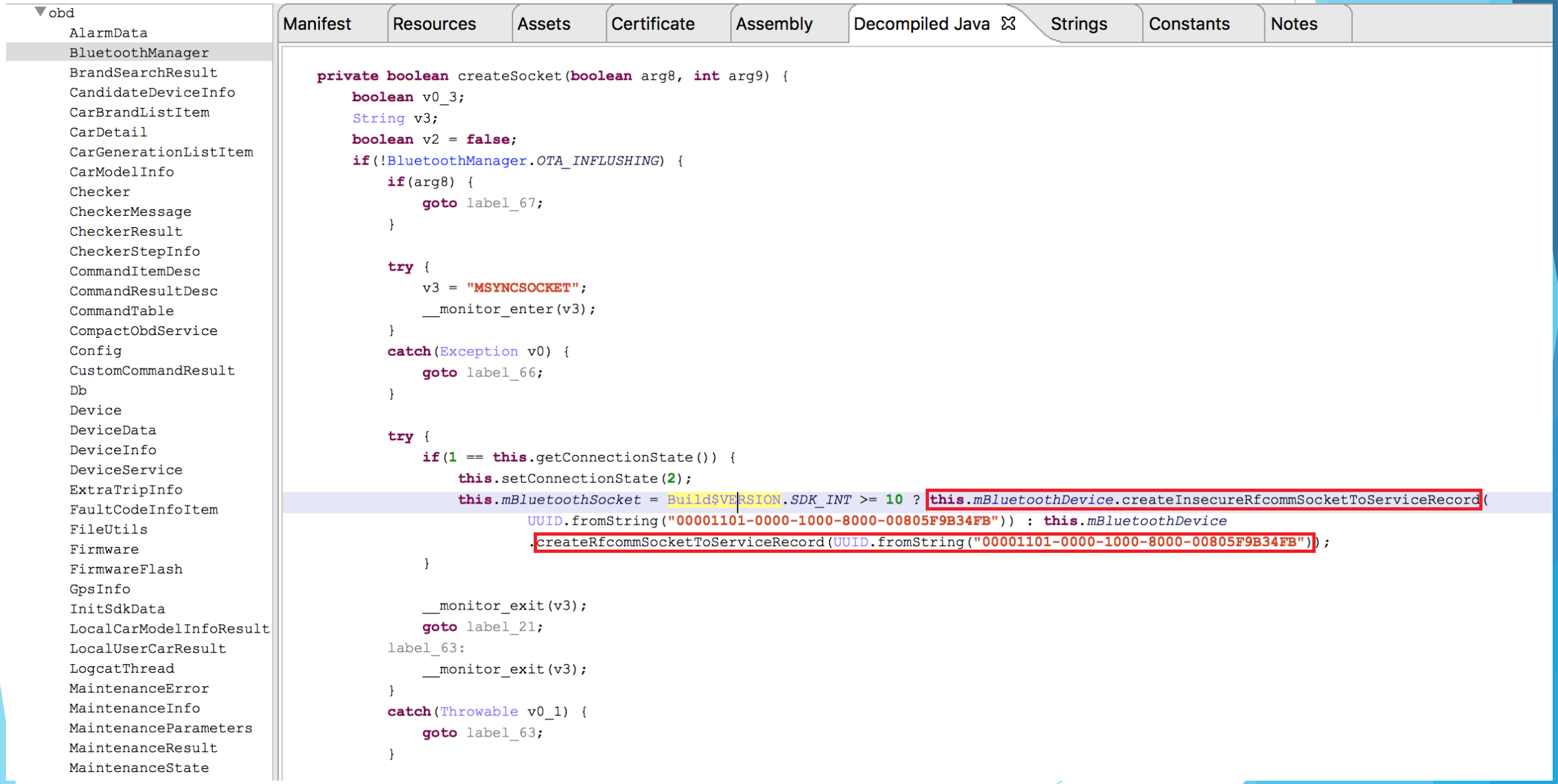

4:03
车辆控制
手机控制车辆


3:44
车辆状态
总里程
549km
续航里程
-
过保里程
0km
过保天数
81天
车窗
天窗


里程 1.1 km
耗时 00:00
停止
已连接(行驶中)
非常健康
123°
11.6V
不支持
12.4
瞬时油耗 L/100km
1.0
83
1984
HUD

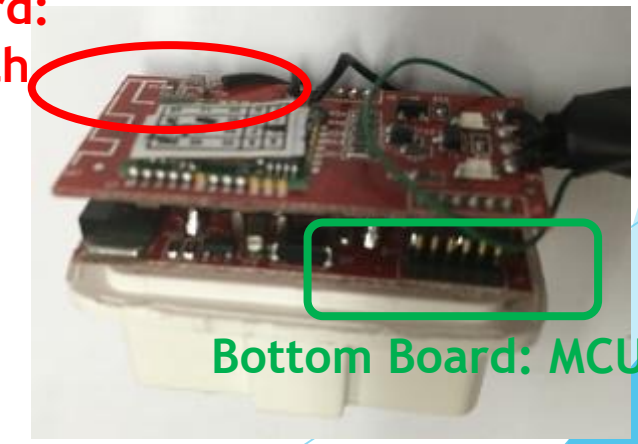

obd
AlarmData
BluetoothManager
BrandSearchResult
CandidateDeviceInfo
CarBrandListItem
CarDetail
CarGenerationListItem
CarModelInfo
Checker
CheckerMessage
CheckerResult
CheckerStepInfo
CommandItemDesc
CommandResultDesc
CommandTable
CompactObdService
Config
CustomCommandResult
Db
Device
DeviceData
DeviceInfo
DeviceService
ExtraTripInfo
FaultCodeInfoItem
FileUtils
Firmware
FirmwareFlash
GpsInfo
InitSdkData
LocalCarModelInfoResult
LocalUserCarResult
LogcatThread
MaintenanceError
MaintenanceInfo
MaintenanceParameters
MaintenanceResult
MaintenanceState
MaintenanceTask
Manager
ManagerParams
MileageSynchonizer
MonthlyCalendar
MonthlyList
MonthlyReport
Manifest
Resources
Assets
Certificate
Assembly
Decompiled Java
Strings
Constants
Notes
public void onProgress(int arg2, int arg3) {
super.onProgress(arg2, arg3);
if(this.val$callback != null) {
this.val$callback.onDownProgress(arg2, arg3);
}
}
public void onSuccess(int arg5, Header[] arg6, File arg7) {
int v3 = 2;
try {
if(Log.isLoggable(LogTag.OTA, 2)) {
Log.d(LogTag.OTA, "string.trim()-->" + Firmware.this.getOTAPath() + " file:"
+ arg7.getAbsolutePath() + " fileisExit:" + arg7.exists());
}
FileUtils.deleteGeneralFile(Firmware.this.getOTAPath());
if(Log.isLoggable(LogTag.OTA, 2)) {
Log.d(LogTag.OTA, " -->> 清除OTA文件夹下的所有文件成功----解压到:-->" + Firmware.this.getOTAPath());
}
FileUtils.upZipFile(arg7, Firmware.this.getOTAPath(), true);
if(this.val$callback != null) {
this.val$callback.onDownResult(20, arg7);
}
Firmware.this.saveLastDown(System.currentTimeMillis());
}
catch(Exception v0) {
if(Log.isLoggable(LogTag.OTA, v3)) {
Log.d(LogTag.OTA, " 解压失败-->> " + v0.getMessage());
}
if(this.val$callback != null) {
this.val$callback.onDownResult(42, arg7);
}
v0.printStackTrace();
}
FileUtils.deleteGeneralFile(arg7.getAbsolutePath());
}
};
No Hardening and No Obfuscation!

Communication Channel



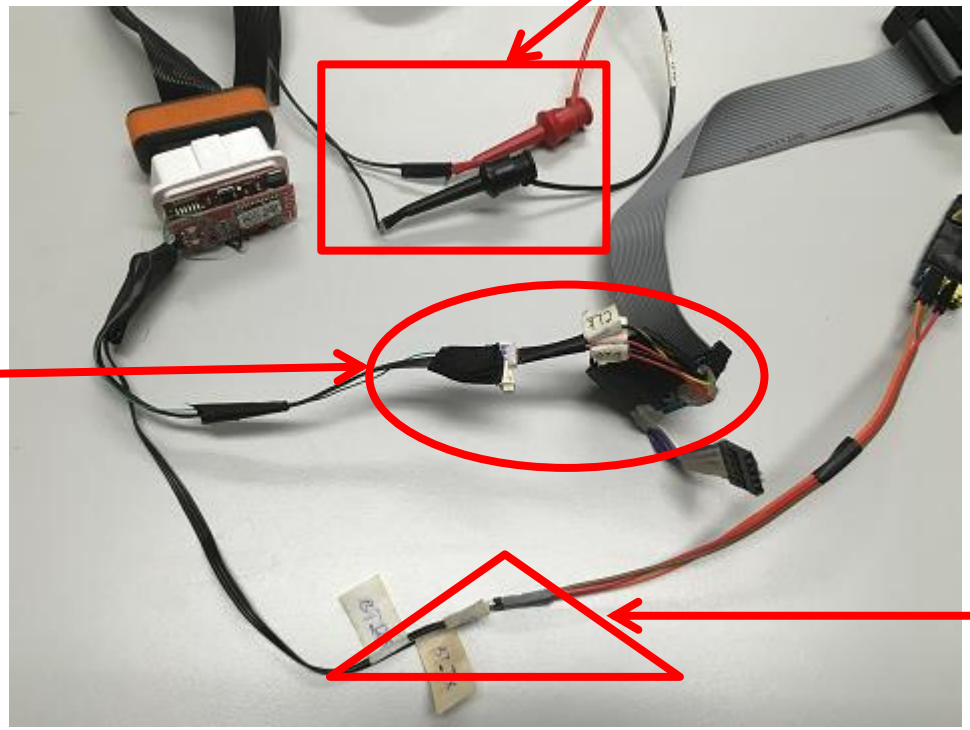
Device

- Microprocessor + Bluetooth + CAN
- No W/R protection
- Communicate with its app through Bluetooth



Device

Monitor CAN Messages



Since the firmware is not protected, we can extract it directly.

Monitor the Communication

CONTENT

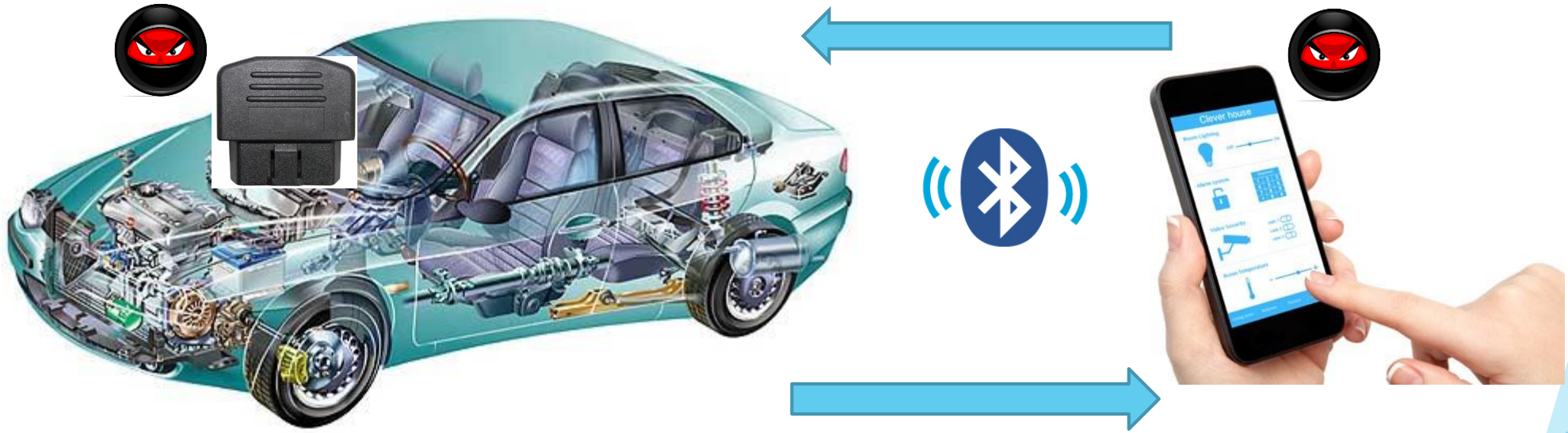
- Telematics and OBD-II
- Attack Surface of Telematics Systems
- A Vulnerable Telematics Device
- Exploit and Attacks
- Securing the Device
- Summary

Exploit

Replace the original firmware with a malicious firmware !

OutputStream.write(byte[])
OutputStream.flush()

Send command



Receive response

InputStream.read()

Woman Follows GPS, Drives Car Into Canada's Georgian Bay

By JULIA JACOBO · May 14, 2016, 12:09 PM ET

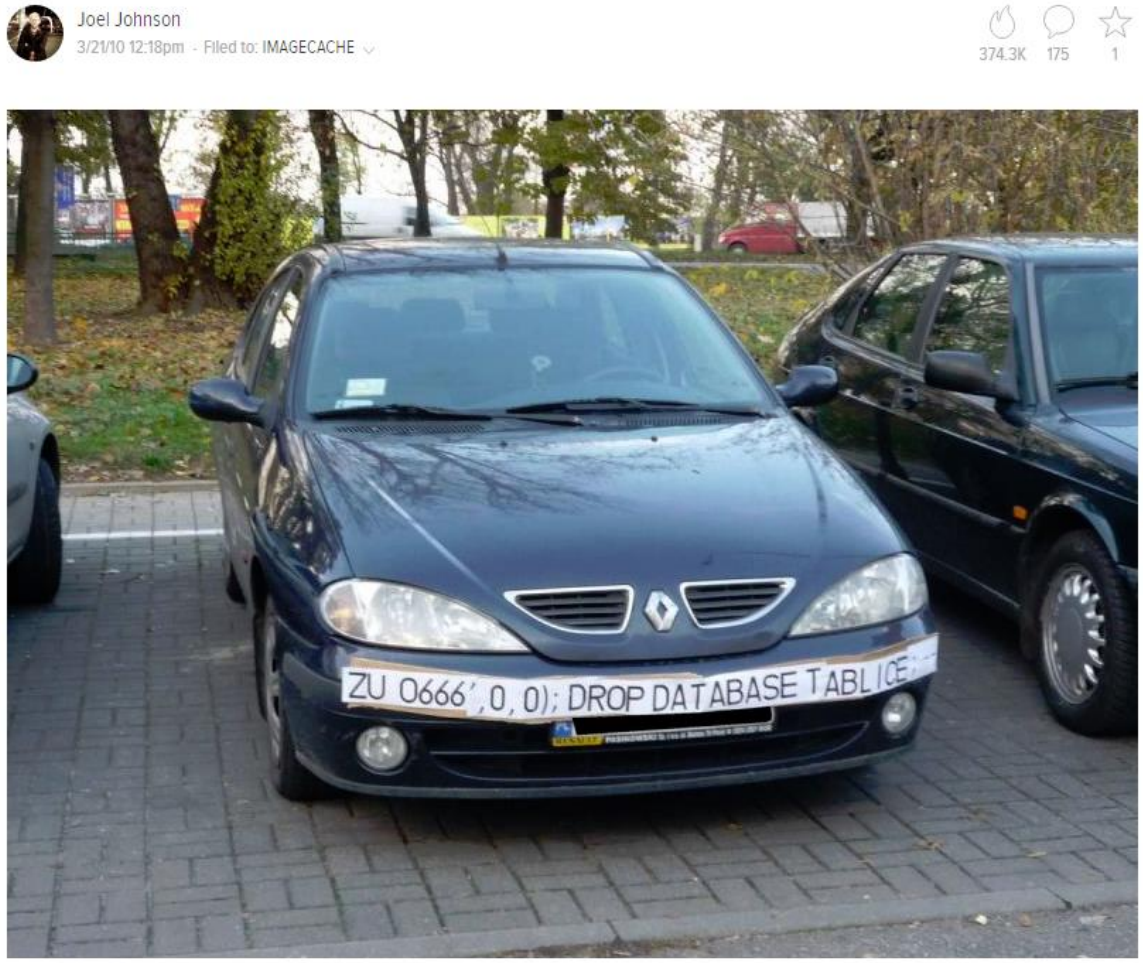
Share with Facebook Share with Twitter

WATCH | Woman Follows GPS, Drives Car Into Canada's Georgian Bay

11K SHARES

Following directions from her car's GPS, a 23-year-old Canadian woman drove straight into a frigid Ontario bay earlier this week.

SQL Injection License Plate Hopes to Foil Euro Traffic Cameras



Experiment Settings

- Volkswagen Magotan 1.8T 2015

- The vulnerable telematics device

- Android smartphone with a PoC attack app

DEMO

CONTENT

- Telematics and OBD-II
- Attack Surface of Telematics Systems
- A Vulnerable Telematics Device
- Exploit and Attacks
- Securing the Device
- Summary

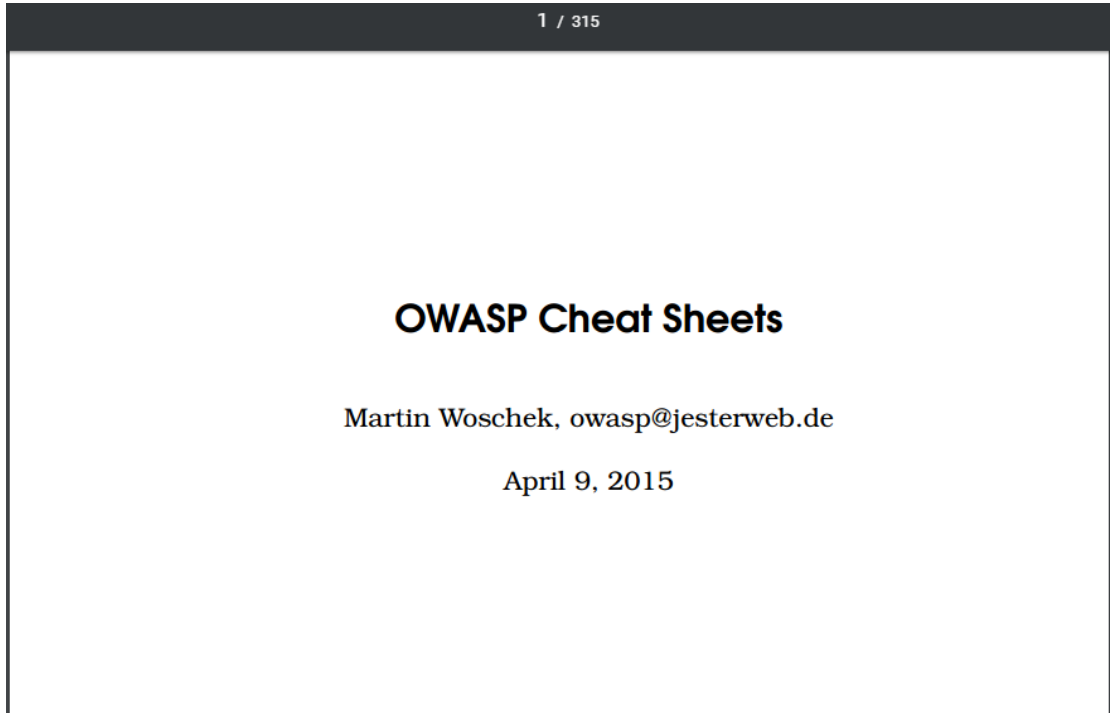
App Security

- Secure data storage
- Secure communication
- Authentication
- Verify the update/firmware downloaded from the backend service
- Obfuscation and hardening
- …

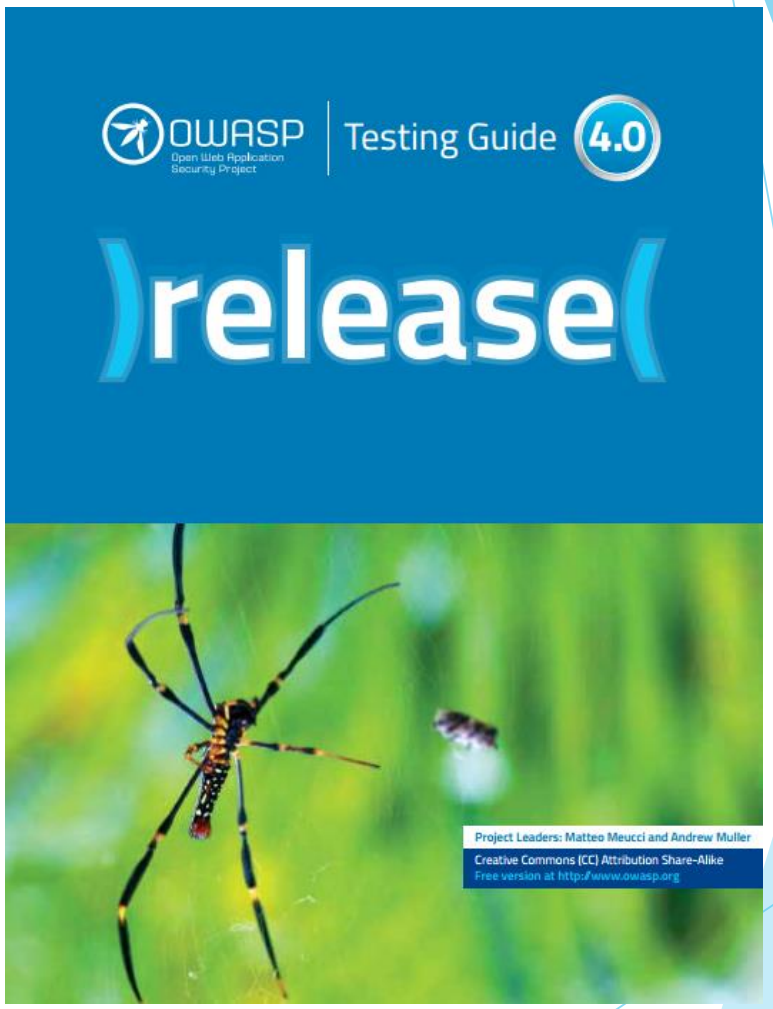
Device Security

- Verify the firmware before installing it
- Protect the existing firmware
- Avoid weak/default passwords
- Encrypt the traffic
- Mutual authentication
- Establish roots of trust
- …

Web Service Security



https://www.owasp.org/images/9/9a/OWASP_Cheatsheets_Book.pdf



https://www.owasp.org/images/1/19/OTGv4.pdf

Summary

- Attack surface of the telematics systems
  - Device
  - Communication
  - App/backend service
- Securing IoT systems
  - Security, safety, reliability, resilience, privacy
  - Monitoring, analysis, and management
- We have been conducting research on mobile security and privacy, network and system security, IoT security, etc.
  - https://www4.comp.polyu.edu.hk/~csxluo/

THANKS!