Tinfoil attack

A study on the security threats and weaknesses of GSM-based communication in BMW cars

Thijs Houtenbos thijs.houtenbos@os3.nl

Jurgen Kloosterman jurgen.kloosterman@os3.nl

February 7, 2013

Introduction

- Evolution of cars
- Mobile communication
- eCall

What security threats are introduced by connecting cars by means of a GSM-module to the Internet and can weaknesses be identified in the implementation in a 2011 BMW 5 Series?

Research target

Background - ConnectedDrive in the Netherlands

Convenience	**Entertainment**	**Safety**
Google local search	News	Manual S.O.S call
Information request	Weather	Automatic S.O.S call
MyInfo	My news	
Send-to-car	Buienradar	
Country information	Office	
BMW Routes	BMW Internet	
Streetview.	Ski sites	
	Snapshots	
	Webcams	

Table : Overview of ConnectedDrive services

GSM in a nutshell

- Network identified by two numbers (MCC/MNC) and a name
- Pre-shared key between provider and SIM-card for encryption
- Network dictates all security parameters

Software used for test network

Open-source software from the Osmocom project[1]

nanoBTS	Radio interface
OpenBSC	Operator systems
OsmoSGSN	Data connectivity in the network
OpenGGSN	Exit point for the data

[1] http://osmocom.org/

Connectivity in the car

- Combox responsible for IVI and connectivity
- Difficult to remove if you are not a BMW mechanic
- Sticker on one of its sides contains some details we wanted

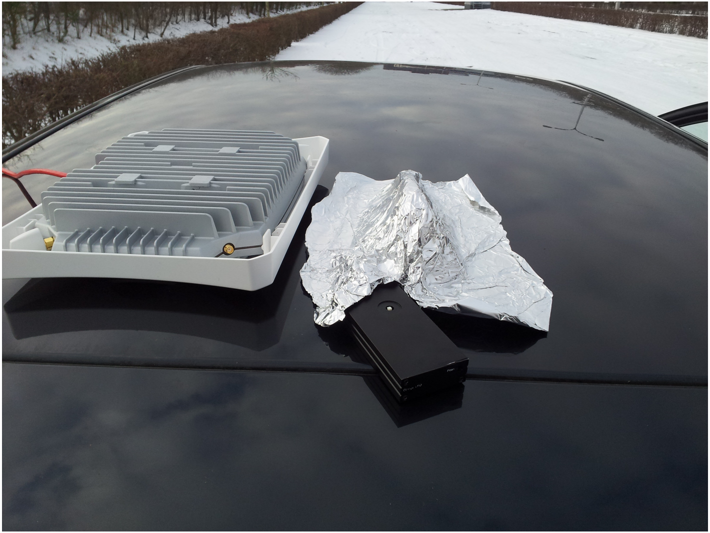
Connectivity in the car

- Initially it was assumed that the provider was Vodafone DE as SIM-number often match the MNC
- Later the IMSI-number revealed the provider to be T-Mobile
- The combox supports the 850, 900, 1800 and 1900MHz frequencies with support for GPRS and EDGE network types

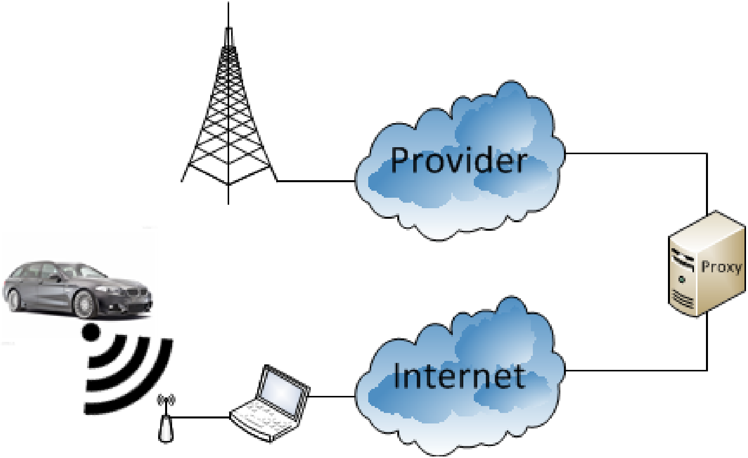
Research - Connection

- Biggest challenge was to let the car connect to test network
- Three attempts needed before result:
  1. Power (fuses, battery, connector)
  2. Block radio spectrum (jammer)
  3. Tinfoil (Faraday cage)

Research - Connection



Research - Connection



Research - Traffic inspection

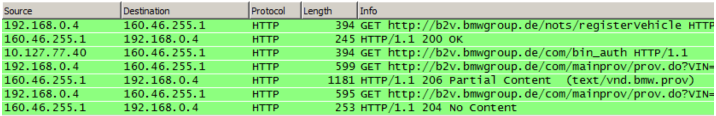
- Traffic between the combox and manufacturer systems is sent with HTTP through a proxy
- Basic authentication is used to authenticate to proxy
- The traffic is compressed to decrease transfer times

Research - Browser

- Car browser is Access NetFront
- User-Agent identifies as Mozilla Firefox 3.5 on Windows 7
- X-Forwarded-For header by proxy reveals internal IP-addresses
- 16-bit range registered with BMW AG, but not advertised on public Internet. Subnet for cars?
- Setup own proxy on their proxy IP to let the browser connect to Internet via us

Research - Registration

- Registration at manufacturer with VIN-number
- Includes own IP and a port accepting connections
- Used to remotely activate services?

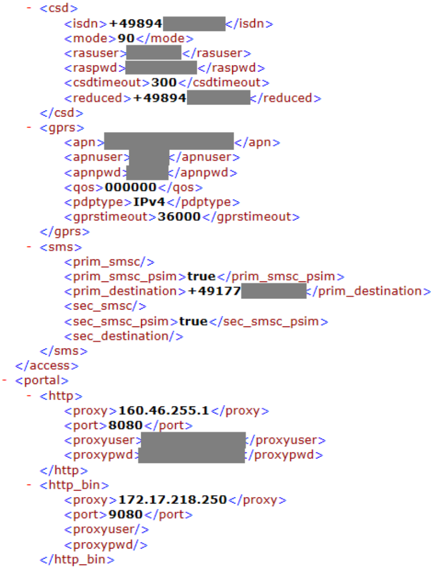


Source	Destination	Protocol	Length	Info
192.168.0.4	160.46.255.1	HTTP	394	GET http://b2v.bmwgroup.de/nots/registerVehicle HTTP
160.46.255.1	192.168.0.4	HTTP	245	HTTP/1.1 200 OK
10.127.77.40	160.46.255.1	HTTP	394	GET http://b2v.bmwgroup.de/com/bin_auth HTTP/1.1
192.168.0.4	160.46.255.1	HTTP	599	GET http://b2v.bmwgroup.de/com/mainprov/prov.do?VIN=
160.46.255.1	192.168.0.4	HTTP	1181	HTTP/1.1 206 Partial Content (text/vnd.bmw.prov)
192.168.0.4	160.46.255.1	HTTP	595	GET http://b2v.bmwgroup.de/com/mainprov/prov.do?VIN=
160.46.255.1	192.168.0.4	HTTP	253	HTTP/1.1 204 No Content

Research - Provisioning

- Provisioning service in the car requests XML-file with settings
- Contains server addresses with port numbers, usernames, passwords and telephone numbers
- Special APN name with login details
- Used by the car to directly connect to the manufacturer?
- The provisioning information is sent compressed but unencrypted. Signed?

Research - Provisioning

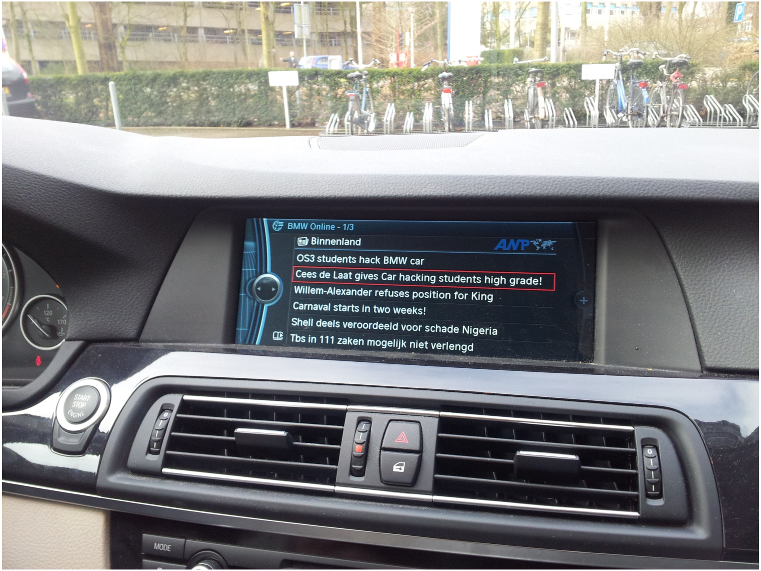


```
    - <csd>
        <isdn>+49894[redacted]</isdn>
        <mode>90</mode>
        <rasuser>[redacted]</rasuser>
        <raspwd>[redacted]</raspwd>
        <csdtimeout>300</csdtimeout>
        <reduced>+49894[redacted]</reduced>
      </csd>
    - <gprs>
        <apn>[redacted]</apn>
        <apnuser>[redacted]</apnuser>
        <apnpwd>[redacted]</apnpwd>
        <qos>000000</qos>
        <pdptype>IPv4</pdptype>
        <gprstimeout>36000</gprstimeout>
      </gprs>
    - <sms>
        <prim_smsc/>
        <prim_smsc_psim>true</prim_smsc_psim>
        <prim_destination>+49177[redacted]</prim_destination>
        <sec_smsc/>
        <sec_smsc_psim>true</sec_smsc_psim>
        <sec_destination/>
      </sms>
  </access>
- <portal>
    - <http>
        <proxy>160.46.255.1</proxy>
        <port>8080</port>
        <proxyuser>[redacted]</proxyuser>
        <proxypwd>[redacted]</proxypwd>
      </http>
    - <http_bin>
        <proxy>172.17.218.250</proxy>
        <port>9080</port>
        <proxyuser/>
        <proxypwd/>
      </http_bin>
```

Research - Applications

- News, weather, sports, etc
- Requested at special server but just HTML
- Again, no encryption just compression
- Setup own webserver with edited news feed and redirected proxy requests

Research - Applications



BMW Online - 1/3

Binnenland

OS3 students hack BMW car

Cees de Laat gives Car hacking students high grade!

Willem-Alexander refuses position for King

Carnaval starts in two weeks!

Shell deels veroordeeld voor schade Nigeria

Tbs in 111 zaken mogelijk niet verlengd

Conclusion

What security threats are introduced by connecting cars by means of a GSM-module to the Internet and can weaknesses be identified in the implementation in a 2011 BMW 5 Series?

- The interesting features are not yet available in NL :(
- Easy to take over network in theory, a lot harder in practice
- No security found in the current systems, but impact is limited

Questions

Thank for your presence. Are there any questions?