IMQ MINDED SECURITY

UN ECE 155 Threats in the real world: Wireless Attacks and Mitigations. A case study

Stefano Di Paola - CTO

AN IMQ GROUP COMPANY

together toward excellence

Agenda

- Introduction to IMQ Minded Security
- Automotive CyberSecurity & UNECE R155
- Choosing a Case Study
- Conclusions

Intro to IMQ Minded Security

- ✓ IMQ Minded Security started their business in 2007 performing Manual Secure Code Review and Web Application Penetration Testing and has lead the OWASP Testing Guide since 2006.

- ✓ Today IMQ Minded Security combines the latest security research with our worldwide recognized testing techniques to meet your business goals and strengthen the security of your products and services.

- ✓ We are living in the era of insecure software, our Software Security Experts can guide you to implement the roadmap for Software Security by Design.

Software Security by Design
BRAKING SYSTEM
SMART TRANSPORTATION
DRIVER ASSISTANT SYSTEM
AUTOMOTIVE
SMART DEVICES
ROBOT AUTOMATION
LOCKERS

IMQ Minded Security Customers & Global Reach

Product and services presence in 17 countries

Industry sectors include:

- Automotive
- Energy
- Banking
- Finance
- Software
- Telecoms
- E-commerce

Who Am I?

- ✓ Stefano Di Paola
- ✓ Seasoned App Sec Expert ~20Yrs
- ✓ CTO & CoFounder @ IMQ MindedSecurity
- ✓ Security Researcher with dozens of new Techniques, Tools & Security Bugs.
- ✓ Vehicle Security & Data Access @EuroNCAP WG
- ✓ Invited speaker at most important CyberSec conferences worldwide

OWASP
Open Web Application Security Project

A Primer on CyberSec Awareness

Attack Example on a Passive Key Entry and Start

Play Me

Courtesy: of KU Leuven COSIC. Original Video link https://www.youtube.com/watch?v=clrNuBb3myE

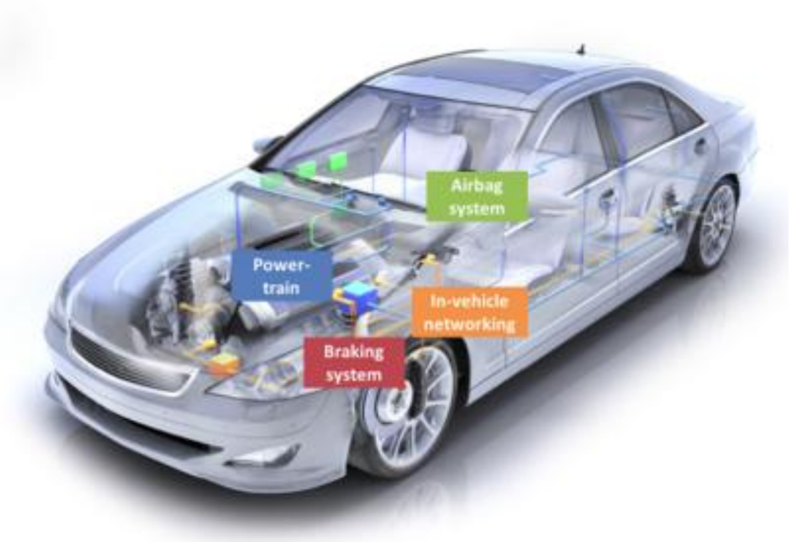
How to Prevent These Scenarios?

Example of Main Threats on PKES

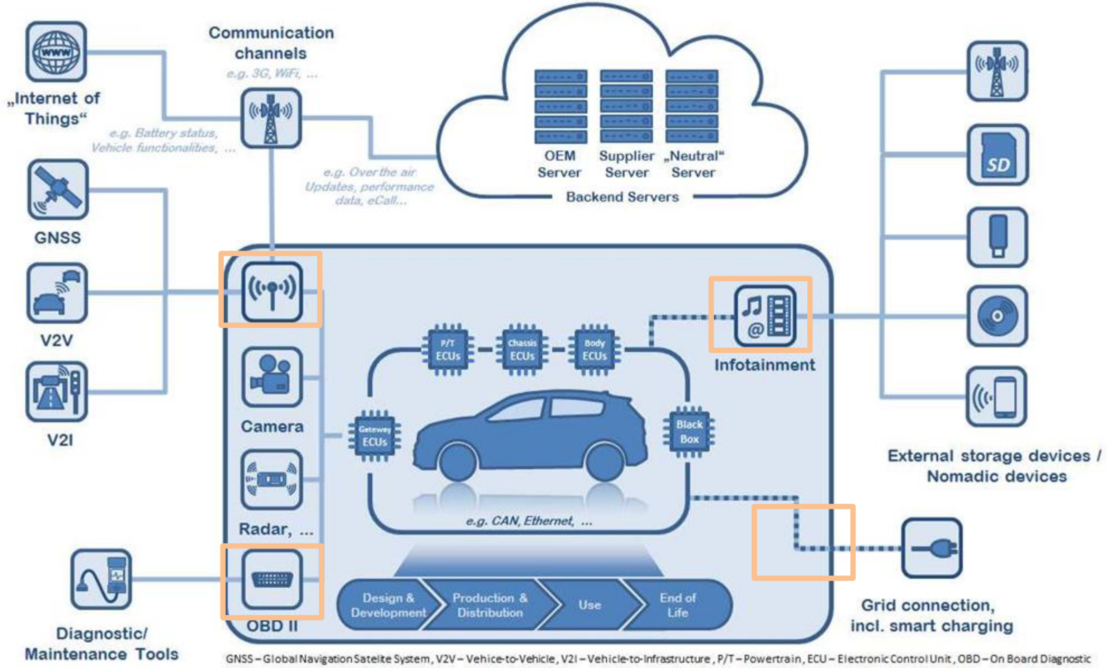
Target	**Threat**	**Attack**	**Mitigation**
Key Fob	Unauthorized FW Update	An **attacker** might try to *abuse the wireless update functionality* to update the PKES with a **malicious FW**	Use a Signed Firmware to confirm **Integrity**
Encryption Keys	Direct Access to Encryption Keys	An **attacker** might *abuse key cloning functionalities* to **impersonate owner**.	Create physical confirmation for **Key Cloning**
…	..	..	..

Automotive Cyber Security

- **Automotive Cyber Security** refers to the branch of **computer security** **focused** on the **cyber risks** related to the **automotive context**.
  - *Not to be confused with automotive safety*.
- Modern automobiles contain over 100 of ECUs (Electronic Control Units) networked together.
- ECUs control several aspects that can harm physical safety.
- They need to be robust and resilient.



Automotive Wireless Attack Surface



GNSS – Global Navigation Satelite System, V2V – Vehice-to-Vehicle, V2I – Vehicle-to-Infrastructure , P/T – Powertrain, ECU – Electronic Control Unit, OBD – On Board Diagnostic

BUT… Modern Cars are not only ECUs.

Entrypoint ECUs

- Passive Anti-Theft System (PATS)
  - Range ~10 cm
- Tire Pressure Monitoring System (TPMS)
  - Range ~1 m
- Remote Keyless Entry/Start (RKE)
  - Range ~5-20 m
- Bluetooth
  - Range ~10 m

Short-range

- Radio Data System
  - Range ~100 m
- DAB+
- Telematics/Cellular/Wi-Fi
  - Range varying but broad
- Internet/Apps

Long-range

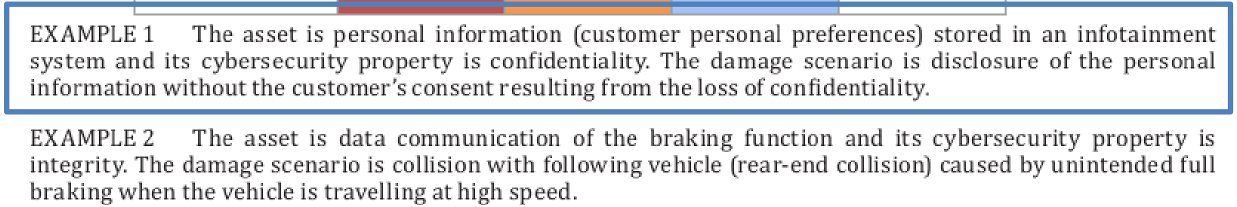
Exposed interfaces:

- WI-FI
- GSM
- CAN Bus
- Encryption Channels
- Bluetooth

Automotive CyberSec Impacts as per ISO21434

When does an issue becomes Security related?

Rating / *Category*	Severe	Major	Moderate	Negligible
Safety				✓
Financial		✓		
Operational			✓	
Privacy	✓			



EXAMPLE 1 The asset is personal information (customer personal preferences) stored in an infotainment system and its cybersecurity property is confidentiality. The damage scenario is disclosure of the personal information without the customer's consent resulting from the loss of confidentiality.

EXAMPLE 2 The asset is data communication of the braking function and its cybersecurity property is integrity. The damage scenario is collision with following vehicle (rear-end collision) caused by unintended full braking when the vehicle is travelling at high speed.

UNECE R155: Introduction

UN REGULATION ON UNIFORM PROVISIONS CONCERNING THE APPROVAL OF VEHICLES WITH REGARDS TO CYBER SECURITY AND CYBER SECURITY MANAGEMENT SYSTEM

- Formalized *Threat Analysis*
- Asks Vendors to **implement** a *Security Process* on several levels
- **Verification** based on a *set of control audits*
- CyberSec Management System (CSMS) shall *cover security aspects* in **every phase**.
    - Development/Production/Post Production

UNECE R155 says that the Vendor Shall

1. Provide Documented proof of deployed CSMS

2. Perform a Specific Threat Analysis on Cars and Services

3. Implement the mitigations

UNECE R155 says that the Vendor Shall

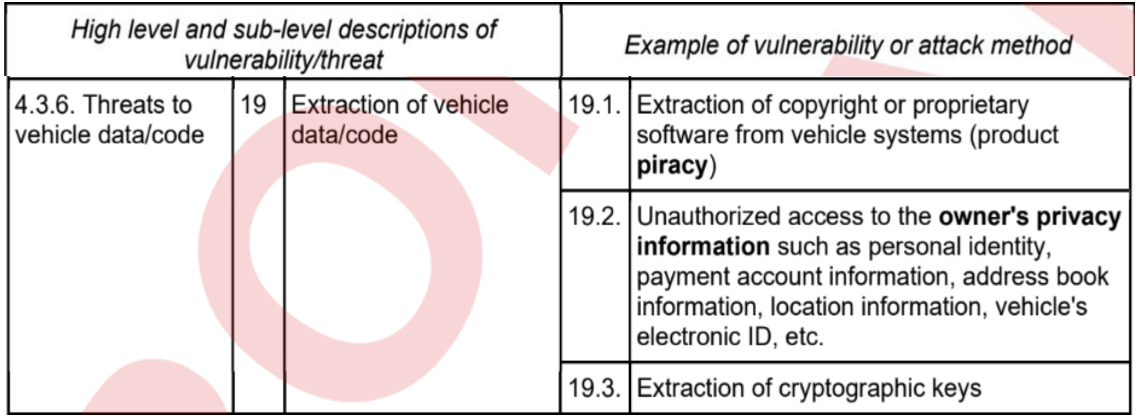
1. Provide Documented proof of deployed CSMS

2. **Perform a Specific Threat Analysis on Cars and Services**

3. **Implement the mitigations**

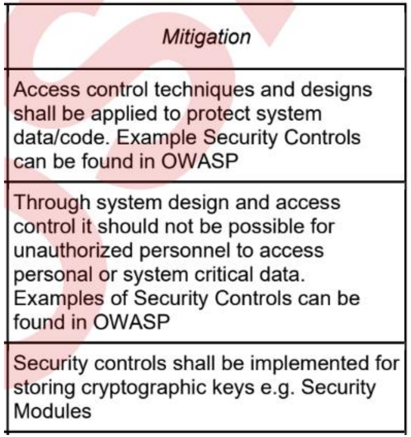
UNECE R155 Proposed Threats

Methodology Based on attack surface and threat analysis + Mitigations



High level and sub-level descriptions of vulnerability/threat			*Example of vulnerability or attack method*	
4.3.6. Threats to vehicle data/code	19	Extraction of vehicle data/code	19.1.	Extraction of copyright or proprietary software from vehicle systems (product **piracy**)
			19.2.	Unauthorized access to the **owner's privacy information** such as personal identity, payment account information, address book information, location information, vehicle's electronic ID, etc.
			19.3.	Extraction of cryptographic keys

Annex A Threats



Mitigation
Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP
Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data. Examples of Security Controls can be found in OWASP
Security controls shall be implemented for storing cryptographic keys e.g. Security Modules

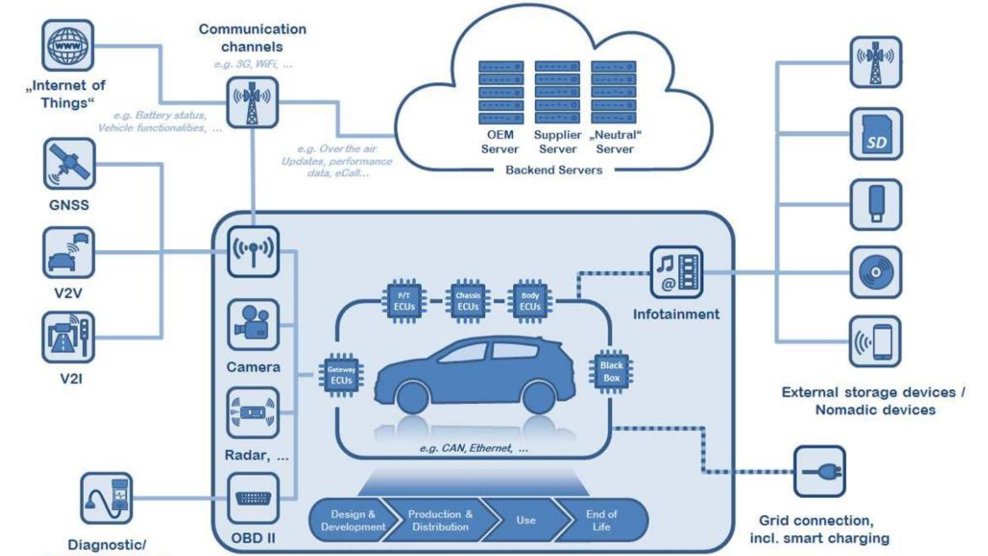
Annex B - Mitigations

Research and Technical Knowledge are the essence of the missing parts:

<u>Test for the correctness of the implemented mitigations</u>.

UNECE R155: Choose a Case Study

Something That Happens to Be on ***Every Car***?



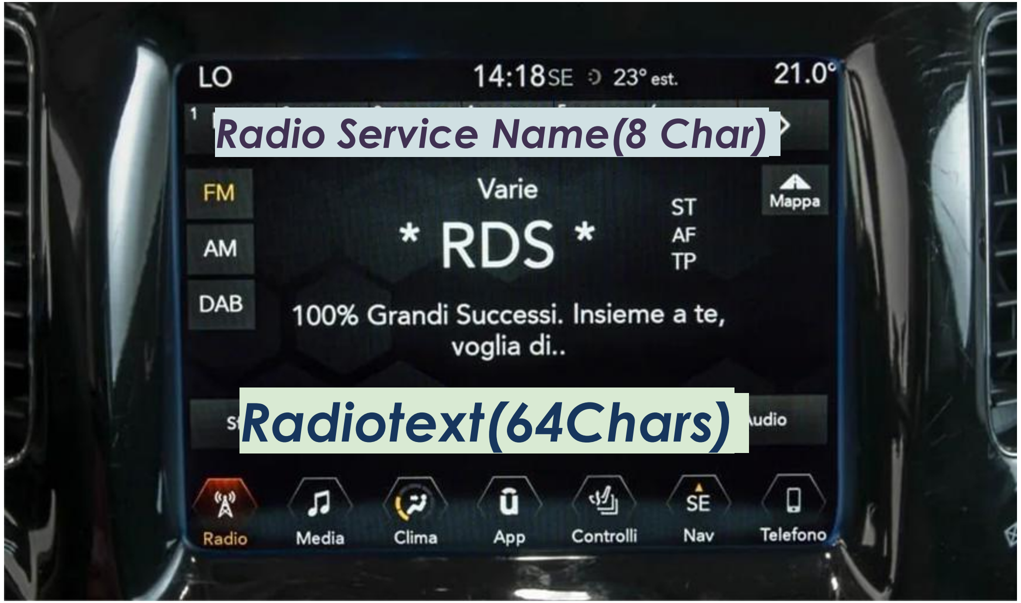
GNSS – Global Navigation Satelite System, V2V – Vehice-to-Vehicle, V2I – Vehicle-to-Infrastructure, P/T – Powertrain, ECU – Electronic Control Unit, OBD – On Board Diagnostic

What about Radio Receivers?

Digital Broadcasting

- Not Only ***Analogue Audio*** but ***Digital Data*** that must be ***Parsed***.
- Opening a door to attack scenarios:
  - ***RDS***: ***Radio Service Name***, ***Radiotext***..
  - ***DAB+***: ***Digital Audio (+Formats)***, ***Images (+Formats)***, ***Interaction*** (***Clickable URLs*** etc..)

RDS Receivers Parse and Render Data



100% Grandi Successi. Insieme a te, voglia di..

Radio Service Name(8 Char)

Radiotext(64Chars)

The RDS Data Specifications https://www.iz3mez.it/wp-content/library/ebook/RDS%20-%20The%20Radio%20Data%20System.pdf

Infotainment - Main Threats On RDS

Target	**Threat**	**Attack**	**Mitigation**
User Interface	Display Message **Spoofing**	An **attacker** might try to *broadcast radiotext messages* over victims frequency	*None. Issue by Design.* ***Obsolete Technology*** *from 1984*
Infotainment OS	**Privilege Escalation** via Rendering Parser Injection	An **attacker** might send *radioText containing characters that are specia*l to the Rendering Engine (HTML Entities)	*Escape Special Characters*
RDS-TMC (Traffic Message Channel)	**Unauthorized** Traffic Messages	An **attacker** might *broadcast alerts* of any kind generating panic over population.	*Use Asymmetric Encryption for TMC*
…	…	…	…

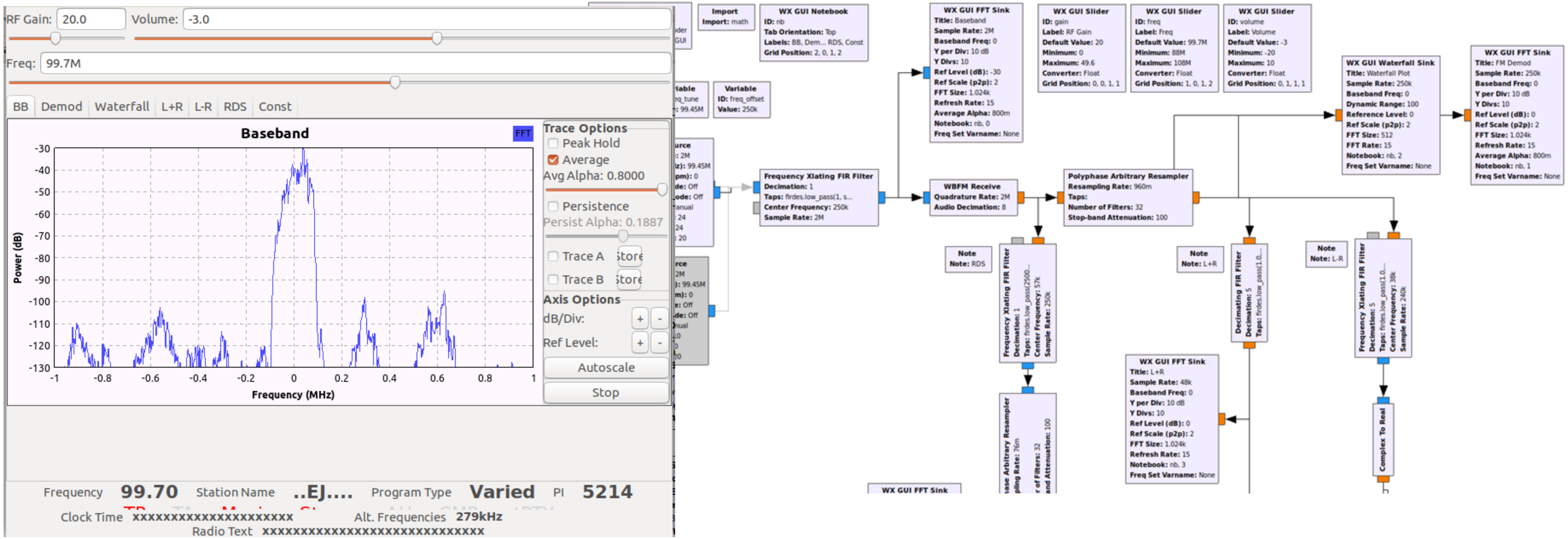
Preparing the Testbed: the RDS Transmitter

Meanwhile @ *IMQ MindedSecurity*
Research Labs...

RDS Transmitter with a RaspberryPi

Preparing the Testbed:

Setting Digital Audio Transmissions



RF Gain: 20.0

Volume: -3.0

Freq: 99.7M

Avg Alpha: 0.8000

Persist Alpha: 0.1887

Frequency 99.70 Station Name ..EJ.... Program Type Varied PI 5214

Clock Time xxxxxxxxxxxxxxxxxxxxxx Alt. Frequencies 279kHz

Radio Text xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Import
Import: math

WX GUI Notebook
ID: nb
Tab Orientation: Top
Labels: BB, Dem... RDS, Const
Grid Position: 2, 0, 1, 2

Variable
ID: freq_offset
Value: 250k

WX GUI FFT Sink
Title: Baseband
Sample Rate: 2M
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): -30
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Average Alpha: 800m
Notebook: nb, 0
Freq Set Varname: None

WX GUI Slider
ID: gain
Label: RF Gain
Default Value: 20
Minimum: 0
Maximum: 49.6
Converter: Float
Grid Position: 0, 0, 1, 1

WX GUI Slider
ID: freq
Label: Freq
Default Value: 99.7M
Minimum: 88M
Maximum: 108M
Converter: Float
Grid Position: 1, 0, 1, 2

WX GUI Slider
ID: volume
Label: Volume
Default Value: -3
Minimum: -20
Maximum: 10
Converter: Float
Grid Position: 0, 1, 1, 1

WX GUI Waterfall Sink
Title: Waterfall Plot
Sample Rate: 250k
Baseband Freq: 0
Dynamic Range: 100
Reference Level: 0
Ref Scale (p2p): 2
FFT Size: 512
FFT Rate: 15
Notebook: nb, 2
Freq Set Varname: None

WX GUI FFT Sink
Title: FM Demod
Sample Rate: 250k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Average Alpha: 800m
Notebook: nb, 1
Freq Set Varname: None

Frequency Xlating FIR Filter
Decimation: 1
Taps: firdes.low_pass(1, s...
Center Frequency: 250k
Sample Rate: 2M

WBFM Receive
Quadrature Rate: 2M
Audio Decimation: 8

Polyphase Arbitrary Resampler
Resampling Rate: 960m
Taps:
Number of Filters: 32
Stop-band Attenuation: 100

Note
Note: RDS

Frequency Xlating FIR Filter
Decimation: 1
Taps: firdes.low_pass(2500...
Center Frequency: 57k
Sample Rate: 250k

Note
Note: L+R

Decimating FIR Filter
Decimation: 5
Taps: firdes.low_pass(1.0,...

Note
Note: L-R

Frequency Xlating FIR Filter
Decimation: 5
Taps: firdes.low_pass(1.0,...
Center Frequency: 38k
Sample Rate: 240k

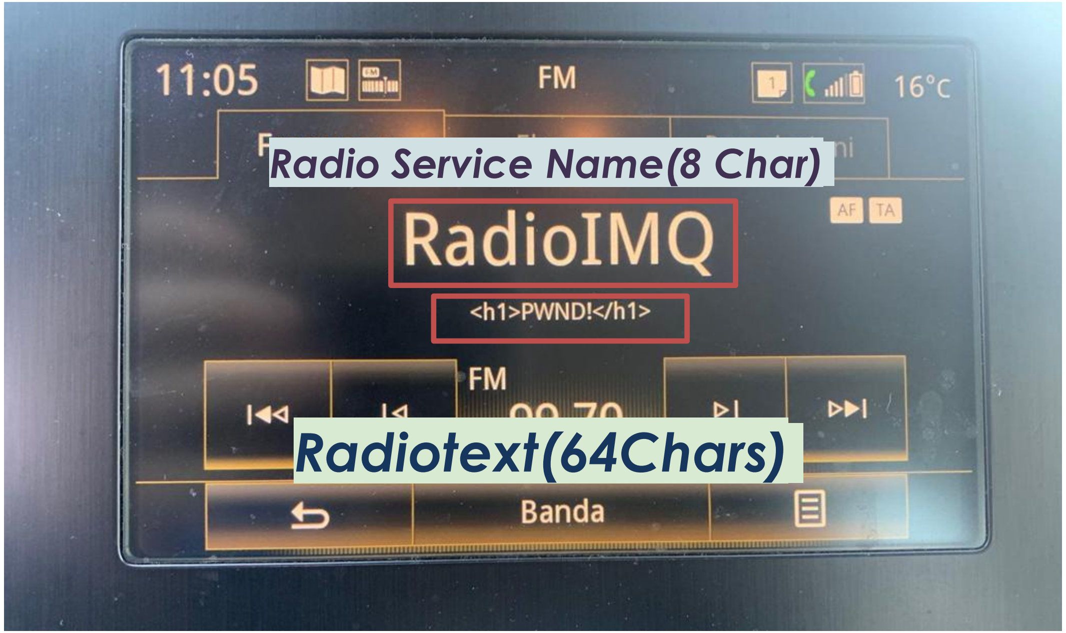
WX GUI FFT Sink
Title: L+R
Sample Rate: 48k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Notebook: nb, 3
Freq Set Varname: None

Complex To Real

By *IMQ MindedSecurity* **Research Labs**

together toward excellence

Attacking & Fooling a Real **RDS** Receiver



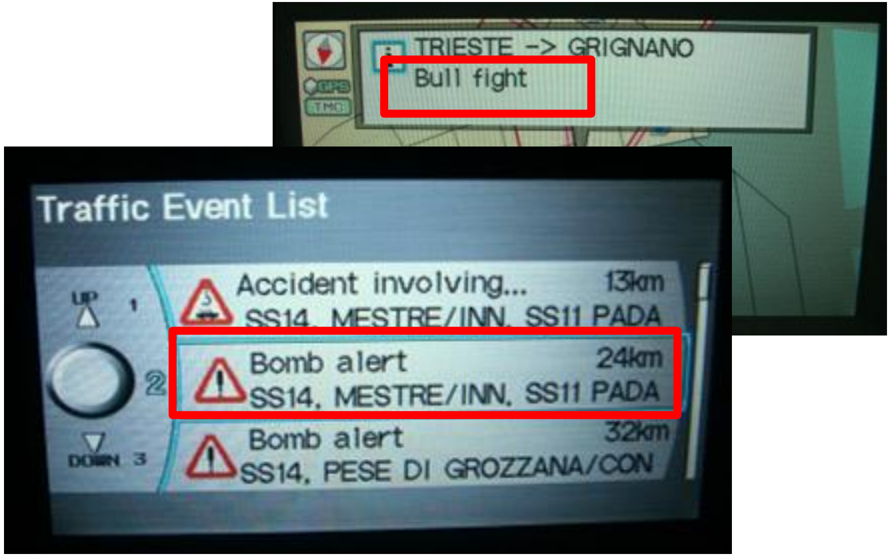
Radio Service Name(8 Char)

Radiotext(64Chars)

By** IMQ MindedSecurity **Research Labs

RDS-TMC Attacks

Demos of Traffic Message Channel Abuses



TRIESTE -> GRIGNANO

Bull fight

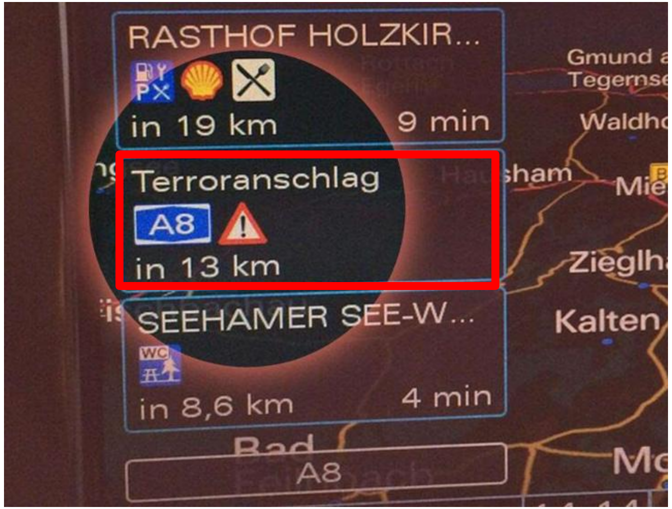
Traffic Event List

Accident involving... 13km
SS14 MESTRE/INN. SS11 PADA

Bomb alert 24km
SS14, MESTRE/INN. SS11 PADA

Bomb alert 32km
SS14, PESE DI GROZZANA/CON

Barisani-Bianco, BlackHat 2007



RASTHOF HOLZKIR...
in 19 km 9 min

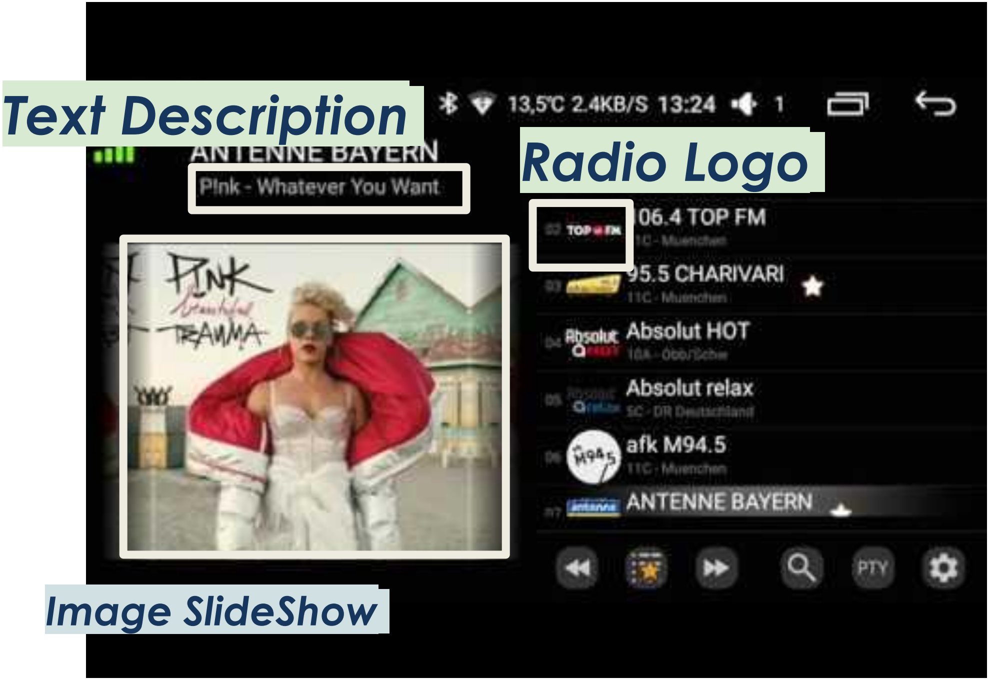
Terroranschlag
A8
in 13 km

SEEHAMER SEE-W...
in 8,6 km 4 min

A8

Bloessl, Fosdem 2015

DAB+ Decoders Parse and Render Data



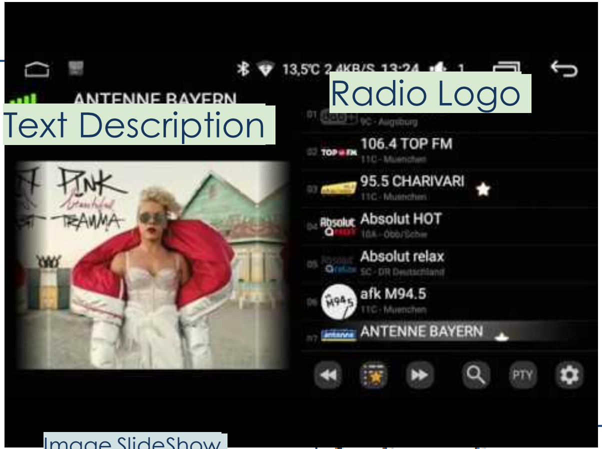
Quite the same as RDS

Right?

DAB+ Data Specifications

https://www.worlddab.org/dab/technical-specifications

DAB+ Attack Surface



Radio Logo

Text Description

Image SlideShow

Data applications

ClickThroughURL

TS 101 499: SlideShow

AlternateLocationURL

TS 102 818: SPI xml

TS 102 371: SPI binary

EPG

TS 103 177: Filecasting

TS 102 980: DL Plus

TS 102 979: Journaline

TS 102 428: DMB

TS 103 551: TPEG

TS 103 689: Filtered Information Service

Data transport coding

EN 301 234: MOT

TS 101 759: TDC

IMG/
OTHER Format

TS 102 427: MPEG-2 TS

Audio coding

TS 102 563: DAB+ audio

TS 103 466: DAB audio

TS 101 757: DAB audio testing

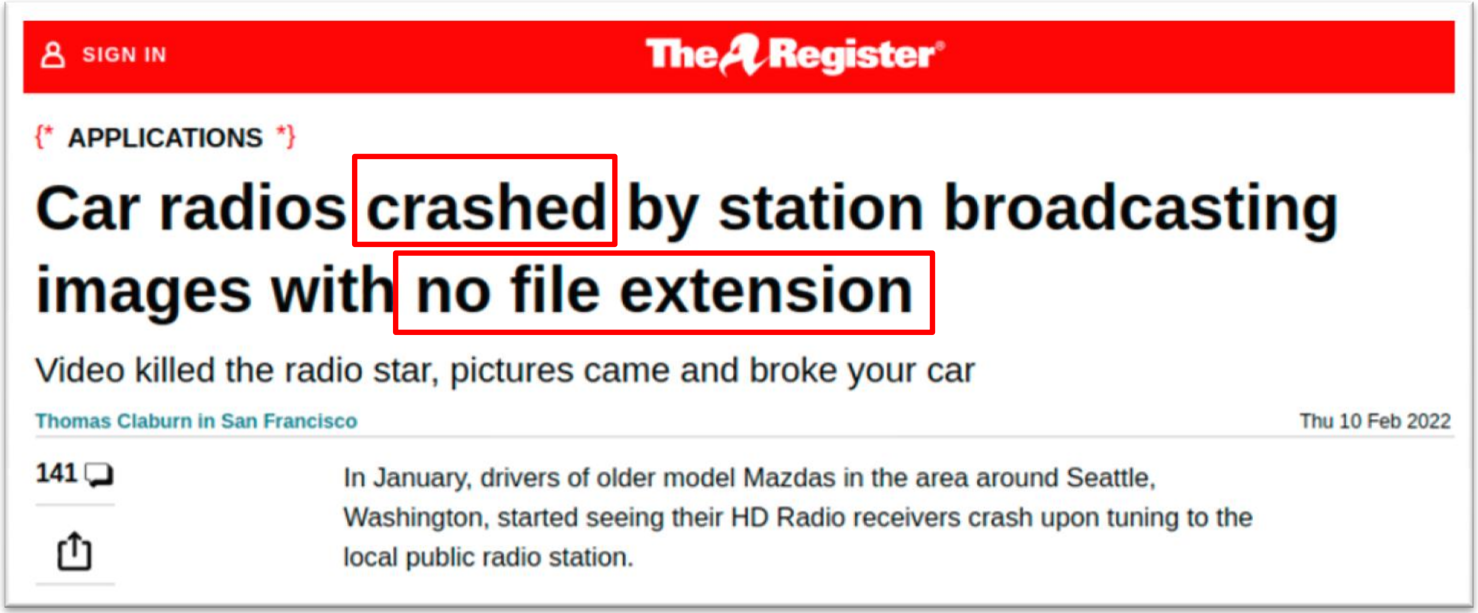
AUDIO Formats

20+ Specifications, 50+ Parsers

DAB+ Data Specifications

https://www.worlddab.org/dab/technical-specifications

DAB+ & Security Bugs



SIGN IN

The Register

{* APPLICATIONS *}

Car radios crashed by station broadcasting images with no file extension

Video killed the radio star, pictures came and broke your car

Thomas Claburn in San Francisco

Thu 10 Feb 2022

141

In January, drivers of older model Mazdas in the area around Seattle, Washington, started seeing their HD Radio receivers crash upon tuning to the local public radio station.

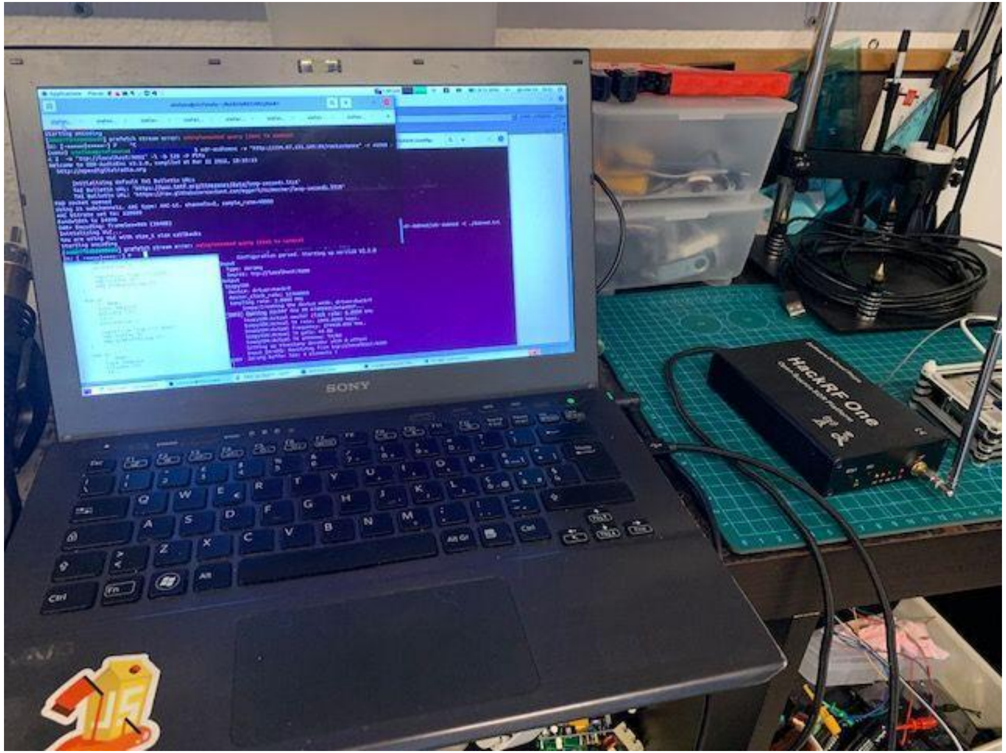
Infotainment - Main Threats On **DAB+**

Target	Threat	Attack	Mitigation
User Interface	Display Message **Spoofing**	An **attacker** might try to *broadcast text messages* over victims frequency	*None. Issue by Design.* ***Obsolete Technologies** from 1997(DAB) and 2007 (DAB+)*
Infotainment OS	**Privilege Escalation** via Rendering Parser Injection	An **attacker** might send *radioText* containing *characters that are special* to the Rendering Engine (HTML Entities)	*Escape Special Characters*
Resources Storage	**Integrity compromission** of DB storage	An **attacker** might broadcast text data containing *special characters* that will result in **SQL Injection**.	*Use prepared Statements or correctly escape special characters.*
Resources Storage	**Integrity compromission** of file storage	An **attacker** might broadcast *image names* containing *special characters* that might fool the application and **overwrite arbitrary files**.	*Escape special characters in File names sent over the air or remove them/use hash.*
…	…	…	…

Preparing the Testbed: **DAB+** Transmitter

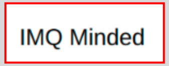
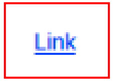
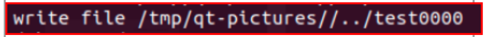
DAB+ Transmitter with:

- HackRF One
- ODR Framework



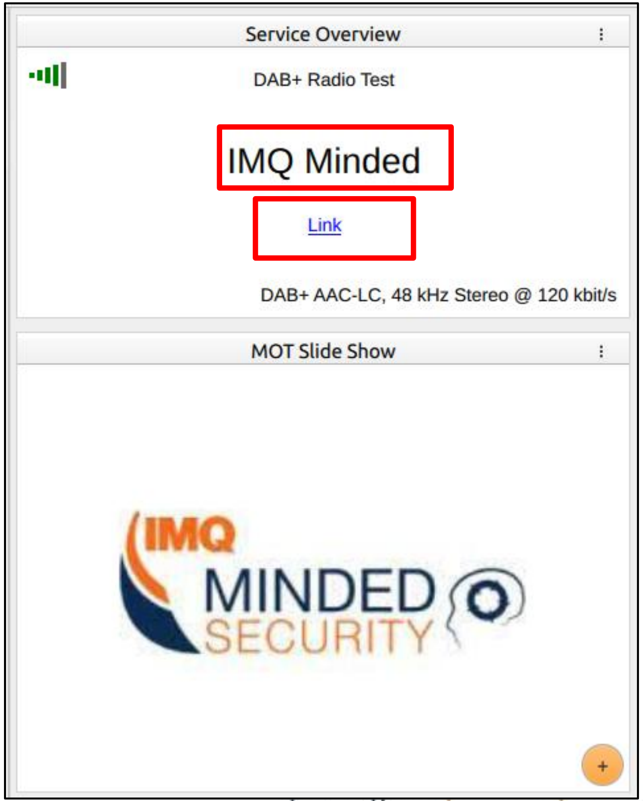
***By** IMQ MindedSecurity*
Research Labs

Infotainment - Attacks On DAB+

Target	Threat	Attack	Successful Attack
User Interface	Display Message **Spoofing**	Force DAB Transmission over existing channels over	See Rendered Spoofed Message on the Display instead of expected Message  IMQ Minded
Infotainment OS	**Privilege Escalation** via Rendering Parser Injection	Set Description with HTML tags: **<a href=”http://www.mindedsecurity.com”> Link</a>**	Shows a rendered link instead of the full text:  Link
Resources Storage	**Integrity compromission** of storage	Send ContentName **../../test0001**	Find a filename out of the expected directory  `write file /tmp/qt-pictures//../test0000`
….	….	….	….

Attacking DAB+ Apps

Infotainment OS	Privilege Escalation via Rendering Parser Injection	Set Description with HTML tags: <a hrf=”http://www.mindedsecurity.com”> Link</a>



Service Overview

DAB+ Radio Test

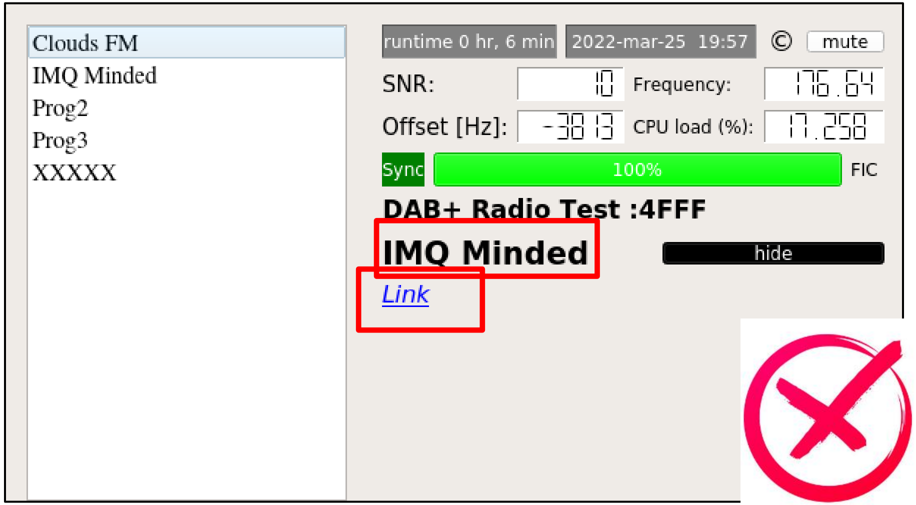
IMQ Minded

Link

DAB+ AAC-LC, 48 kHz Stereo @ 120 kbit/s

MOT Slide Show

Attacking DAB+ Apps



Clouds FM
IMQ Minded
Prog2
Prog3
XXXXX

runtime 0 hr, 6 min | 2022-mar-25 19:57 | © | mute

SNR: 10 Frequency: 176.64

Offset [Hz]: -3813 CPU load (%): 17.258

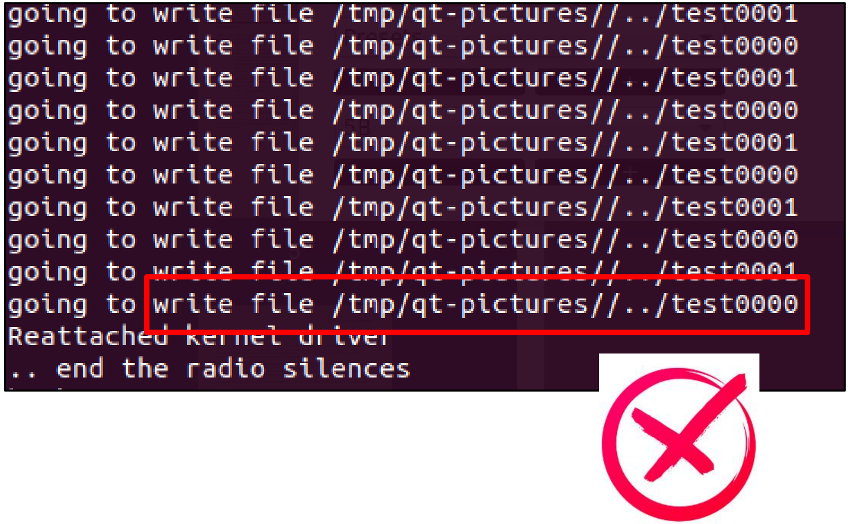
Sync 100% FIC

DAB+ Radio Test :4FFF

IMQ Minded

hide

Link



```
going to write file /tmp/qt-pictures//../test0001
going to write file /tmp/qt-pictures//../test0000
going to write file /tmp/qt-pictures//../test0001
going to write file /tmp/qt-pictures//../test0000
going to write file /tmp/qt-pictures//../test0001
going to write file /tmp/qt-pictures//../test0000
going to write file /tmp/qt-pictures//../test0001
going to write file /tmp/qt-pictures//../test0000
going to write file /tmp/qt-pictures//../test0001
going to write file /tmp/qt-pictures//../test0000
Reattached kernel driver
.. end the radio silences
```

Infotainment OS	**Privilege Escalation** via Rendering Parser Injection	Set Description with HTML tags: **<a href=”http://www.mindedsecurity.com”> Link</a>**
Resources Storage	**Integrity compromission** of storage	Send ContentName **../../test0001**

Conclusions

- Threat Analysis on **DAB+** revealed that it has a quite ***large attack surface***.
- Some **DAB+** **application** is **affected** by specific attacks with *security impacts*.
- **Attackers** can **use** *infotainment* systems to gain control **from remote to local network**.
- **But…**

Conclusions

- Applying UNECE R155 & ISO 21434 Methodology will help to:
  - *Shift security left*
  - *Define a repeatable process*
  - *Make attacks harder*
- **Make it right** and **it will give you back**!

- **DAB+** still need some (Security) attention!

THANK YOU FOR YOUR ATTENTION