C-ROADS CZECH REPUBLIC
MEMBER OF C-ROADS PLATFORM

Co-financed by the European Union
Connecting Europe Facility

SECURITY – not only new buzzword

…we design our future, we implement C-Roads…

O2 Czech Republic
Ing. Jiří Vítek

safety

or / and ?

security

…today

safe road

safe car

secure car

secure road

today…

Security perimeter

RISK LOG

1) INPUT FORGERY

Available ITS units provides OPEN API accessable via WiFi – high security RISK.
Mitigation: limited number of OBU until 2020 for pilot phase, do not use for full-scale deployment.

OBU (embedded) – possibility of CAN bus data forgery, unsecured input
Mitigation: upgrade to new generation of bus; SW OBU must validate the input, the SW must not only forward data but must validate and aggregate messages. Necessity to log processes.

OBU (aftermarket) – unsecured OBD II connector, ExLap interface,
Mitigation: SW OBU must validate the input, the SW must not only forward data but must validate and aggregate messages. Necessity to log processes.

RVU (mobile units) – unsecured proprietary interface,
Mitigation: SW OBU must validate the input, the SW must not only forward data but must validate and aggregate messages. Necessity to log processes.

Virtual OBU (mobile application) – equipment which generates and receives data, must follow all C-ROADS security requirements

General mobile or web application – not generates any data to the system, not necessary to follow all C-ROADS security requirements

RSU (road/highway) – data forgery from sensor and MX control unit, BT/WiFi sensors
Mitigation – see SW RSU must validate the input, the SW must not only forward data but must validate and aggregate messages. Necessity to log processes.
RSU (cities) – data forgery from controller,
Mitigation – physical security
RSU (RLX) – data forgery only from binary inputs,
Mitigation – physical security

Back-office – data forgery from external systems
Mitigation: network security at the level of data providers (if there is not possible to sign each message)

2) SW APPLICATION FORGERY

OBU – possibility of FW forgery
Mitigation: physical security

RSU – possibility of SW/FW forgery
Mitigation: physical security, tamper-proof (intrusion detection and key deletion)

Mitigation: covered by tools of mobile OS, it is necessary to check jail-break and availability secure element (HSM)

Back-office – possibility of SW/FW forgery
Mitigation: physical security

3) HW COMPONENTS SUBSTITUTION

OBU
See SW application forgery.

RSU
See SW application forgery.

4) PHYSICAL SECURITY DISRUTION

Mitigation: intrusion detection, key deletion

5) PRIVATE KEY LEAKAGE

Mitigation: HSM

6) NETWORK COMMUNUCATION ATTACK

Mitigation: communication via public network must be encrypted and signed (only ITS-G5 will be only signed)

7) SOCIAL ENGINEERING

Out of scope of C-ROADS project.

8) FREQUENCY BAND JAMMING / DoS ATTACK

Mitigation: OBU must follow requirements of appropriate standards (declared by the manufacturers – certificate of plug tests)

credibility

…way to succeed

1. to have simple solution = to be reliable
2. to have one solution = to be interoperable
3. to have secure solution = to be credible

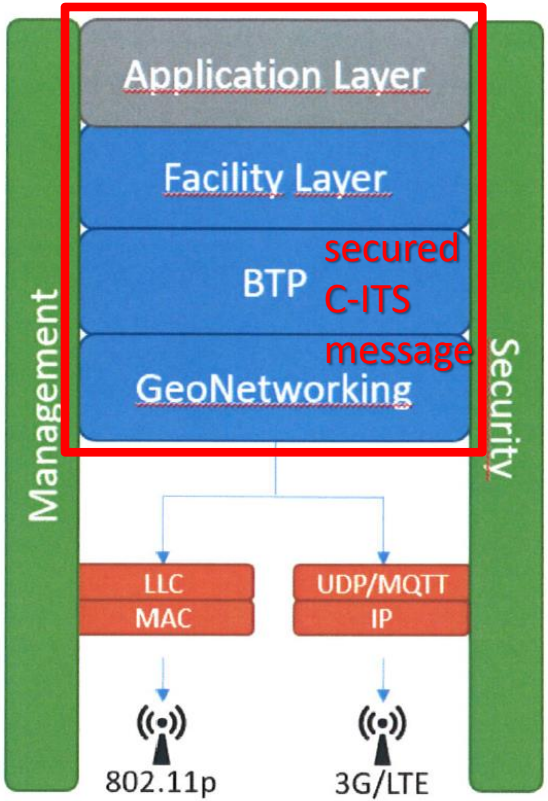
…one message standard, single trust domain

Currently

ETSI ITS standards for ITS-G5 communication

Security has to be performed with the GeoNetworking protocol at the ITS networking & transport layer

(designed only for short-range communication)



Newly

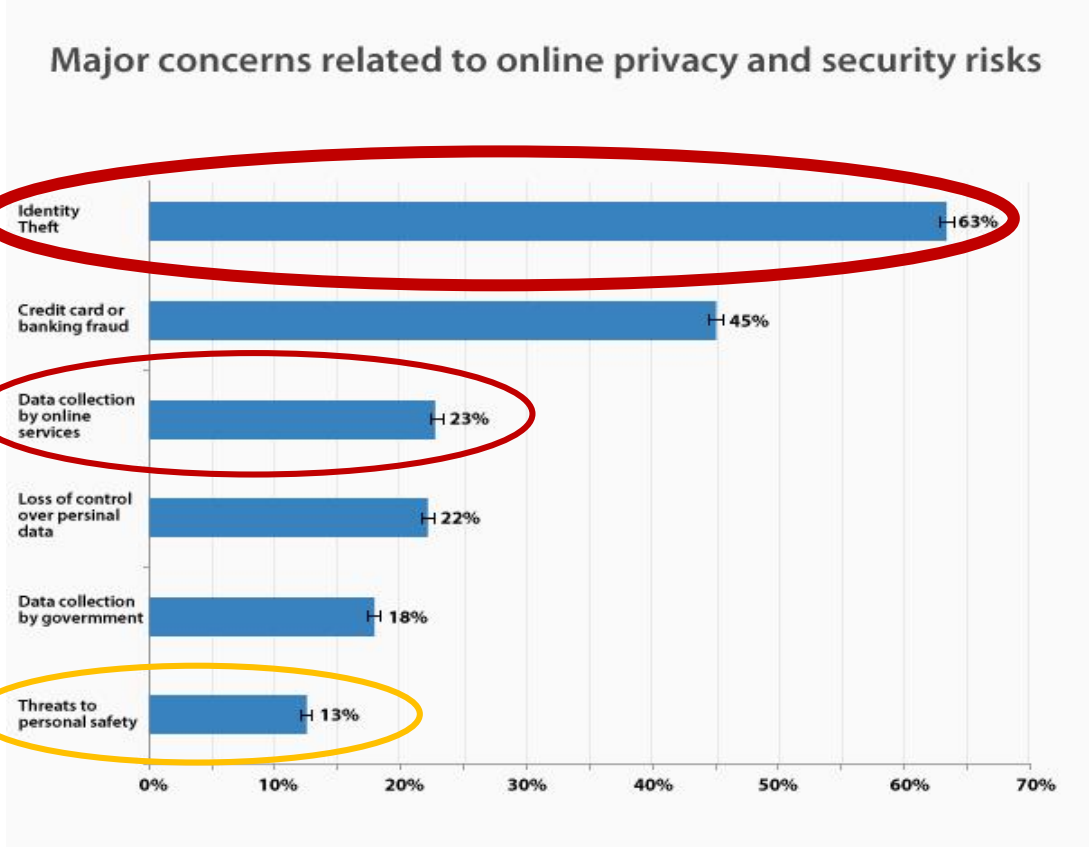
Hybrid communication

<u>Re-use existing standard</u>

+ one standard
+ easy resend and broadcast
+ no re-signing (original message from the source)
- each actor has to have C2X stack

privacy

Perception of data processing systems



Data processing analysis

Data relation matrix

Member	Actor	Message	Relation (communicates with)
MDČR	N/A	N/A	N/A
ŘSD ČR	RSU, OBU, RVU, BO	CAM, DENM, IVI, MAP, SPAT	O2, BKOM, INTENS, ŠKODA, TMCZ, AŽD
SŽDC	N/A	N/A	N/A
AŽD	RSU, BO	CAM, DENM	O2, BKOM, INTENS, ŠKODA, TMCZ, ŘSD
O2	CA, OBU, MA, BO, IntP	CAM, DENM, IVI, MAP, SPAT	BKOM, INTENS, ŠKODA, TMCZ, AŽD, ŘSD
TMCZ	(MA), BO	CAM, DENM, IVI	O2, BKOM, INTENS, ŠKODA, AŽD, ŘSD
BKOM	RSU, OBU, (RVU), BO	CAM, DENM, IVI, MAP, SPAT	O2, INTENS, ŠKODA, TMCZ, AŽD, ŘSD
INTENS	RSU, OBU, BO	CAM, DENM, IVI, MAP, SPAT	O2, BKOM, ŠKODA, TMCZ, AŽD, ŘSD
ČVUT	OBU	CAM, DENM, IVI, MAP, SPAT	O2, ŘSD ČR, AŽD, TMCZ, BKOM, INTENS
ŠKODA	OBU, BO	CAM, DENM, IVI, MAP, SPAT	O2, ŘSD ČR, TMCZ, BKOM, AŽD, INTENS

Messages and private data markers

- Integrační platforma vazba se týká všech partnerů, kteří mají BO

CAM
- Hlavička:
  - Protocol version, Message ID, **Generation time**
- Tělo:
  - **Station ID**, Mobile ITS station, Private ITS station, Physical relevant ITS station => tělo
  - Latitude, Longitude, Elevation, Heading =>**Reference position**
- **Certifikát** - podpis celé zprávy
- **Tučně jsou kritické parametry z pohledu OOÚ**

DENM
- Hlavička:
  - Protocol version, Message ID, **Generation time**
- Tělo:
  - Action ID, Data version, Reliability, Expirity time, Frequency, Is negation
  - Situation, Severity
  - **Latitude, Longitude, Elevation**
  - Trace ID, Waypoint
- **Certifikát**
- **Tučně jsou kritické parametry z pohledu OOÚ**

IVI
- Z pohledu OOÚ nezávadná zpráva v rámci portálu

MAP/SPAT
- Stejný princip, jako IVI

- Je třeba se tedy zaměřit na CAM a DENM zprávy

Generování zpráv
- CAM => MA, OBU, RVU
- DENM = > MA, OBU, RSU, RVU, BO, IntP
- Nosič osobní informace je CAM nebo DENM zpráva generovaná z MA, OBU, RVU
  - Závadu způsobuje všude, kudy tato zpráva poteče
- Identifikován problém při přeposílání (vysílání) DENM zprávy - týká se OBU, které informaci zachycují a vysílají dále. OBU při příjmu zprávu zpracuje a pošle jí dál. Tyto OBU nejsme schopni pojmenovat a identifikovat
- Přeshraniční testování - zahraniční partner musí vždy "nahlásit" úmysl testování na daném území, tím pádem můžeme s konkrétním testerem podepsat předem smlouvu

Ing. Jiří Vítek
O2 Czech Republic
+420602719394
vitek.j@o2.cz

Thank you.

C-ROADS CZECH REPUBLIC
MEMBER OF C-ROADS PLATFORM