Cyber security in V2X communications

Gilles Ampt – 5 December 2017

Chairman of Security Community
Smart Mobility Standards & Practices

Cyber security in V2X communications

Gilles Ampt
security@ditcm.eu

5 December 2017

Topics to be discussed today

- What is Vehicle Security?
- What is V2X Security?
- What are the main risks in V2X?
- WHEN and HOW to address V2X risks?
- How about a trusted V2X communications network?

Holland.

Dutch Smart Mobility Community for Standards & Practices

- Objective: acceleration of the implementation and large scale deployment of Smart Mobility.
- Central place in the Netherlands for knowledge sharing and decision making.
- Involvement of experts and policy makers from governments, industry and research institutions.
- National governance connected to international platforms.

Holland.

FORTUNE SUBSCRIBE

NEWS | POPULAR | VIDEOS | FORTUNE 500

Security Experts Say That Hacking Cars Is Easy JANUARY 26, 2016

FBI's iPhone Crack Has Scared You Silly 11:23 AM EDT

One Woman's Audacious Plan to Create Germany's First Female Astronaut 11:22 AM EDT

NASA Wants You to Design its New Logo 11:14 AM EDT

Microsoft's Surface Phones Could Be Pushed Back to 2017 11:06 AM EDT

Exclusive: These Are the 50 Fastest-Growing Women-Owned Businesses 11:04 AM EDT

These Are the Most Popular ESports Games on Twitch 11:00 AM EDT

Ikea Embraces Virtual Reality With Virtual Kitchen 10:57 AM EDT

Security Experts Say That Hacking Cars Is Easy

by Jonathan Vanian ©JonathanVanian JANUARY 26, 2016, 6:47 PM EDT

New car features come at a cost

SPONSOR CENTER

Automobiles may be getting more advanced, but that

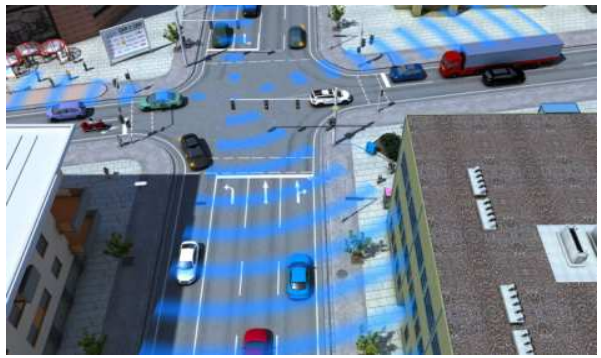
What is Security?
Being in Control of Risks

- Risks of Connected Vehicles
  - Vehicle theft (digital attack)
  - Motor management manipulation (unauthorized remote control)
  - Data loss (incl. loss of personal data/ privacy)
  - Software updates (reliability, authorization)

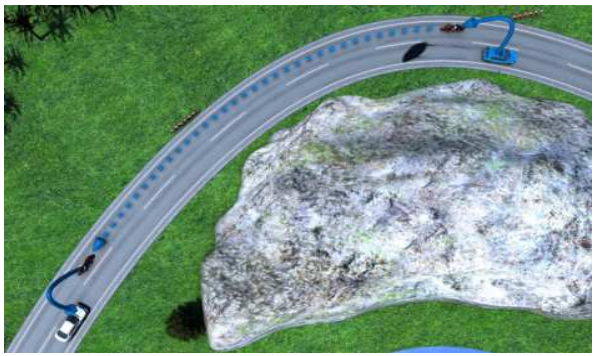
- *Application interests at risk:*
  - *Integrity of data*
  - *Confidentiality of data*
  - *Availability of data*
  - *Authorised Access and Authenticated Access*

Connected driving part of Autonomous driving

Emergency Vehicle

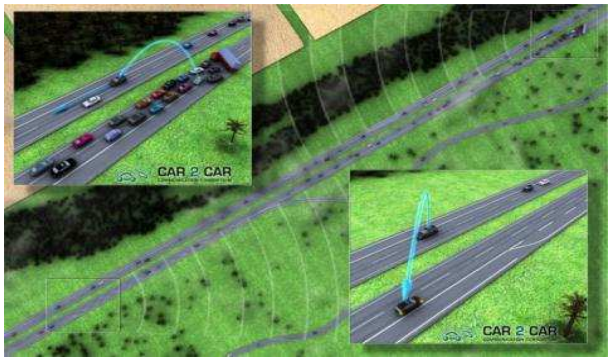


Green Light Optimal Speed Advisory



Hazardous Location Warning

Warning Lights on



Avoidance of traffic jams

Local Road Works Warning

CAR 2 CAR
COMMUNICATION CONSORTIUM

Holland.

Initial risks in V2X communications

Threats	Likelihood/ Impact/ Risk assessment	(ETSI) design requirement/ Organisation Measure
GNSS jamming and spoofing	critical	Monitoring. Robust design e.g. dGPS
Radio signal jamming	critical	Radio frequency agility and control
Message saturation	critical	Message frequency control and Authentication
Replay of expired/ old messages	critical	Message timestamps

Source: ETSI TR 102 893 v1.1.1 (2010)

When and how to address risk?

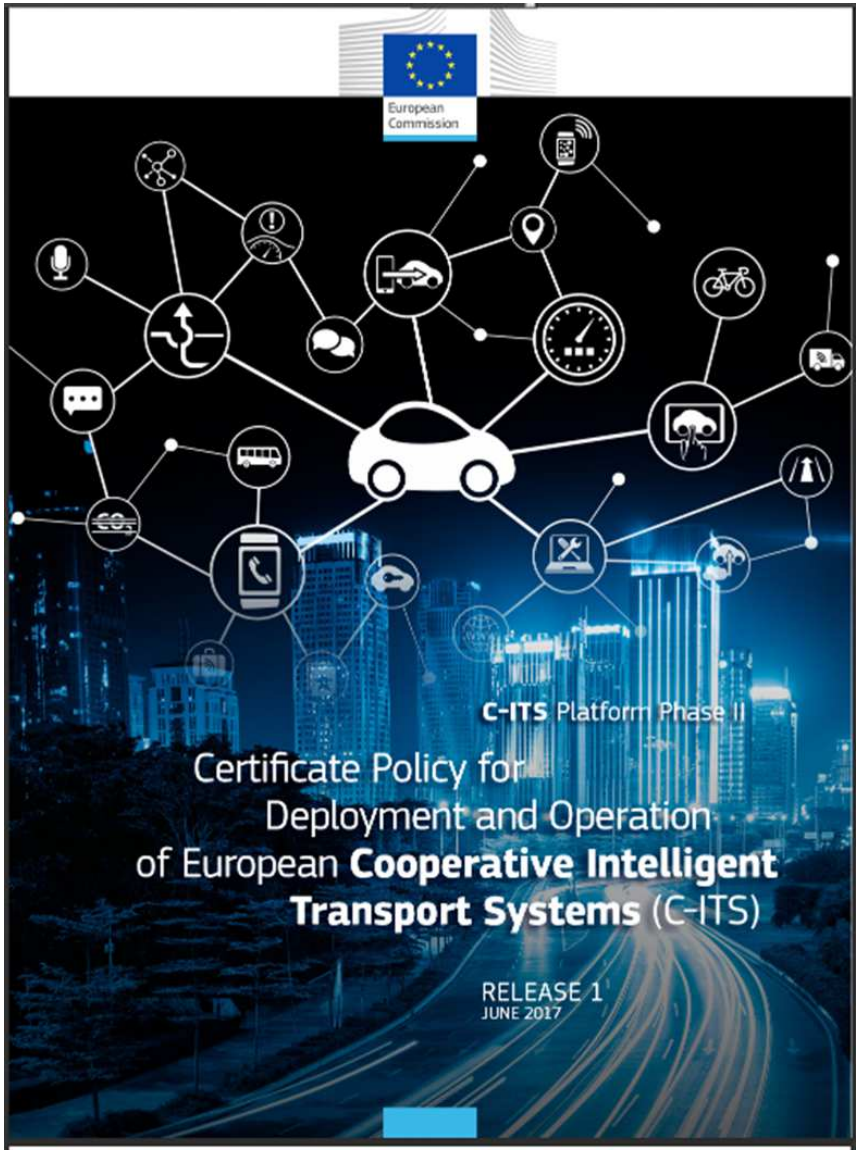
- Risk ownership
  - delegation of risk would be window dressing
- Risk assessment
  - repeatedly needed as risk landscape is evolving

- Legal compliance
  - New EU privacy law (GDPR) demands risk based approach
- Security baselines
  - Stakeholders require organisations to be in control

- V2X *communications*
  - Security by design

Risk is a management process

Risk is a choice *of management*



Security by Design

- EU trust framework for V2X communications
- Authentication and authorisation of ITS stations
  - Commercial vehicles
  - Special purpose vehicles
  - Road side units

Holland.

Cyber security in V2X communications

Gilles Ampt
security@ditcm.eu

5 December 2017