Security Challenges for Cooperative and Interconnected Mobility Systems

Date: 17 September 2013
Tjerk Bijlsma, Sander de Kievit, Jacco van de Sluis,
Ellen van Nunen, Igor Passchier and Eric Luiijf

TNO innovation for life
DITCM
Dutch Integrated Testsite Cooperative Mobility

Contents

- Context
- Attack Incentives
- Mobile Internet Connections
- Vehicular Ad Hoc Networking
- In-Vehicle Systems
- Discussions
- Conclusions

TNO innovation for life

Context: Trends

Automotive innovation in software

(estimate is that this will be 80%*)

- More microprocessors and sensors in the vehicle

Increased connectivity

- Telematics systems by Kia, Daimler and BMW
  - Integrate map-based, vehicle diagnostics, and e-call (mandatory as of 2015)
- Interfaces: internet or ad hoc networks
- Interconnected in-vehicle systems

UVO eServices – KIA

MBRACE2 – Daimler

BMW ConnectedDrive – BMW

* R.N. Charette, "This car runs on code", IEEE spectrum, Feb. 2009

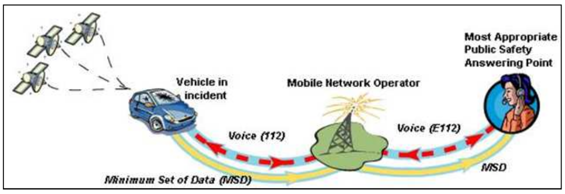
Context: Cooperative and Interconnected mobility systems

- Cooperative Driving results in*:
  - Less traffic congestion
  - Less traffic accidents
  - Less CO_2 emission

mobility: cooperative driving

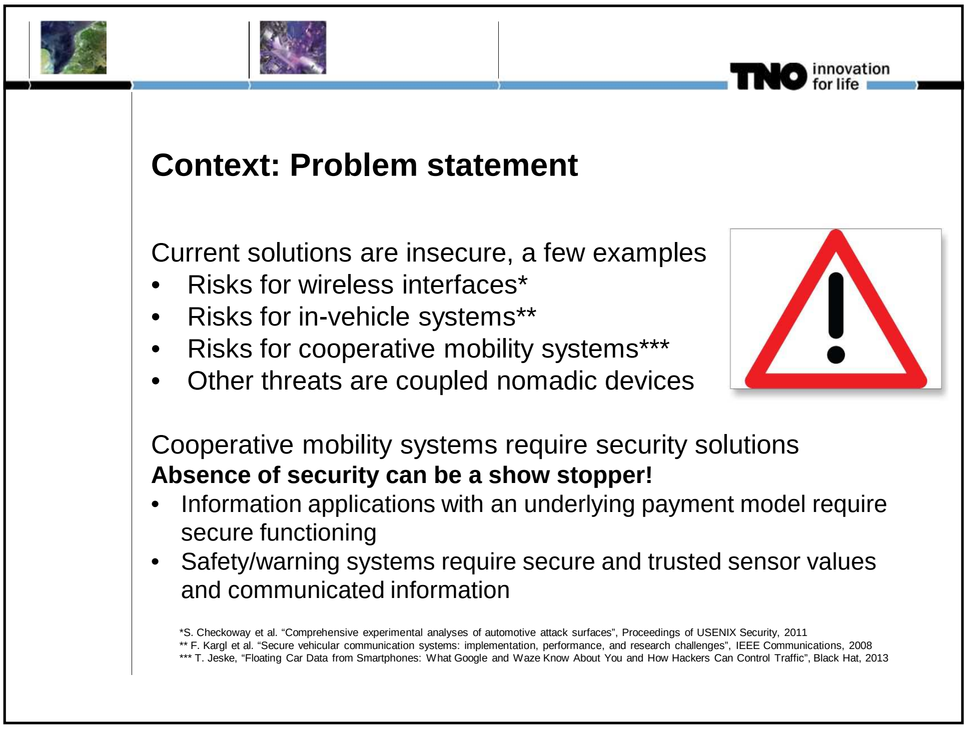
safety: collision warning → mitigation → avoidance

comfort: cruise control, advanced cruise control, speed advice


Vehicle in incident
Mobile Network Operator
Most Appropriate Public Safety Answering Point
Voice (112)
Voice (E112)
MSD
Minimum Set of Data (MSD)

safety: e-call system

*TNO report 2008-D-R0996/A: "Smarter and better – the benefits of intelligent traffic"



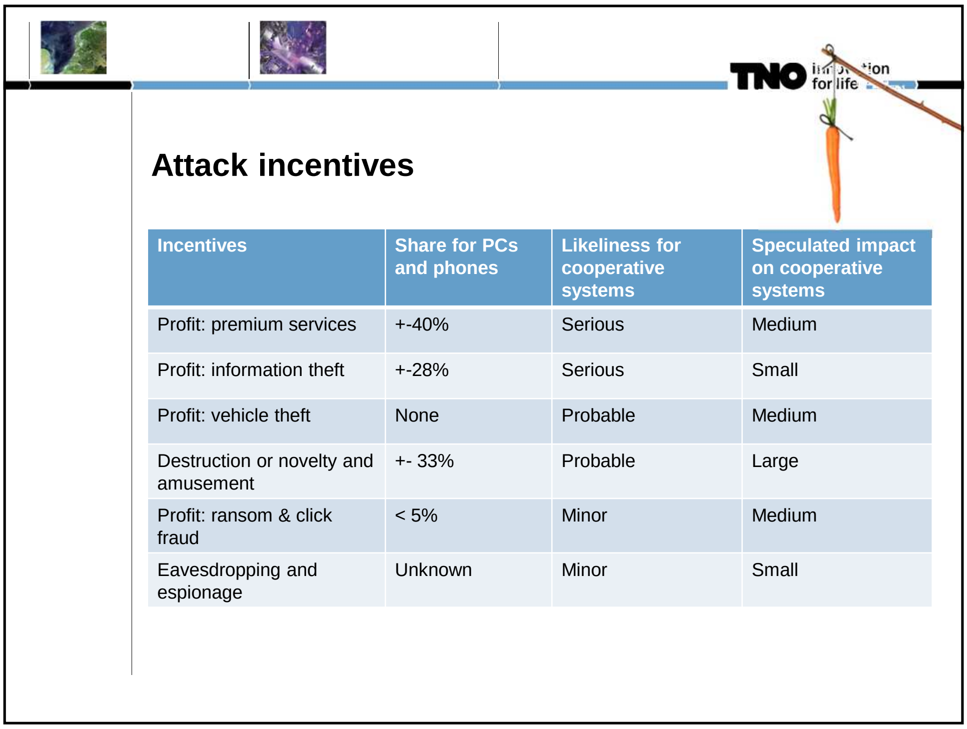
TNO innovation for life

Context: Problem statement

Current solutions are insecure, a few examples
- Risks for wireless interfaces*
- Risks for in-vehicle systems**
- Risks for cooperative mobility systems***
- Other threats are coupled nomadic devices

Cooperative mobility systems require security solutions
Absence of security can be a show stopper!
- Information applications with an underlying payment model require secure functioning
- Safety/warning systems require secure and trusted sensor values and communicated information

*S. Checkoway et al. "Comprehensive experimental analyses of automotive attack surfaces", Proceedings of USENIX Security, 2011
** F. Kargl et al. "Secure vehicular communication systems: implementation, performance, and research challenges", IEEE Communications, 2008
*** T. Jeske, "Floating Car Data from Smartphones: What Google and Waze Know About You and How Hackers Can Control Traffic", Black Hat, 2013



TNO innovation for life

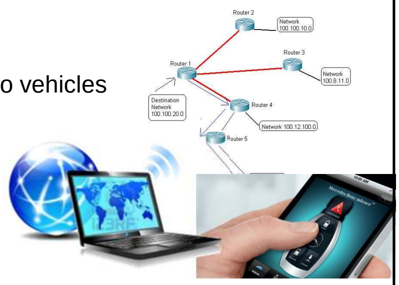
Attack incentives

Incentives	Share for PCs and phones	Likeliness for cooperative systems	Speculated impact on cooperative systems
Profit: premium services	+-40%	Serious	Medium
Profit: information theft	+-28%	Serious	Small
Profit: vehicle theft	None	Probable	Medium
Destruction or novelty and amusement	+- 33%	Probable	Large
Profit: ransom & click fraud	< 5%	Minor	Medium
Eavesdropping and espionage	Unknown	Minor	Small

Mobile internet communication

Problems and solutions

- Always-on data-connections added to vehicles
  - Update software
  - Real-time routing information
  - Web browsing
  - Remote vehicle control



Security risk factors

- An internet uplink opens up previously closed systems
  - Safety critical system becomes vulnerable
  - Potential to harm national security
  - Long life cycle poses a challenge that is unrivalled by IT devices

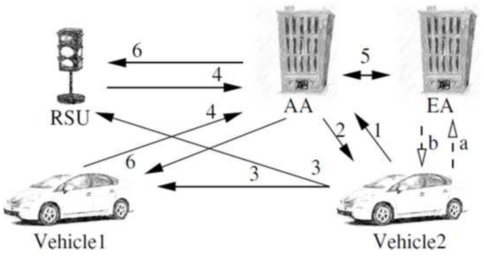
Vehicular Ad Hoc Networking

Problems and solutions

- Rapidly changing topology and unorganized nature
- ETSI performed a vulnerability and risk factor analysis in 2010
  - Counter measures and improvements formulated
- Certificate based communication are proposed

Security risk factors

- Data integrity
- Insecure positioning
- Response latency



TNO innovation for life

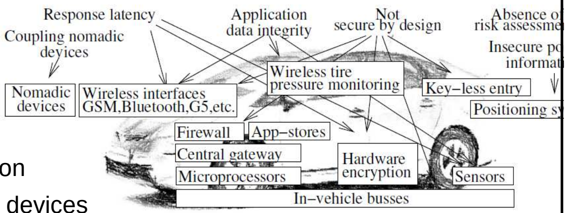
In-Vehicle Systems

Problems and solutions

- Hardware encryption modules
- Firewalls
- Software upgradeable
- Coupling with nomadic systems

Security risks

- Secure by design
  - Ductile
  - Graceful degradation
- Coupling of nomadic devices
- Lack of risk factor analysis



TNO innovation for life

Discussion

Dilemmas

- Data protection vs. information sharing
- Private sector vs. public sector
- Stimulate the economy vs. improve the security

Organizational challenges

- Education in cyber hygiene for maintenance
- OEMs should prepare for massive recalls
- Change of vehicle safety laws
- Backward compatibility between algorithms
- Log behaviour for accountability
- Licence revocation might be needed

Conclusions

Security for interconnected and cooperative mobility systems will become important in the coming year

- Crucial for acceptance and successful introduction of cooperative mobility systems

- Most serious incentive is profit
  - Biggest threat is destruction and novelty
- Biggest security risk factors
  - Application data integrity validation
  - Insecure positioning
  - Systems are currently not secure by design
- Dilemmas and organizational challenges should be addressed

Questions?

tjerk.bijlsma@tno.nl