Social robots, Autonomous vehicles and the Internet of Things.

Cybersecurity and Data Privacy Aspects.

GIUSEPPE LUGANO, PETER HOLEČKO & **MARTIN HUDÁK (PRESENTER)**

UNIVERSITY OF ŽILINA, SLOVAKIA

MARTIN.HUDAK@ERACHAIR.UNIZA.SK

WORKSHOP "AI LOVE YOU", POTSDAM 8 DECEMBER 2017

About the ERAdiate project
(University of Žilina, Slovakia)

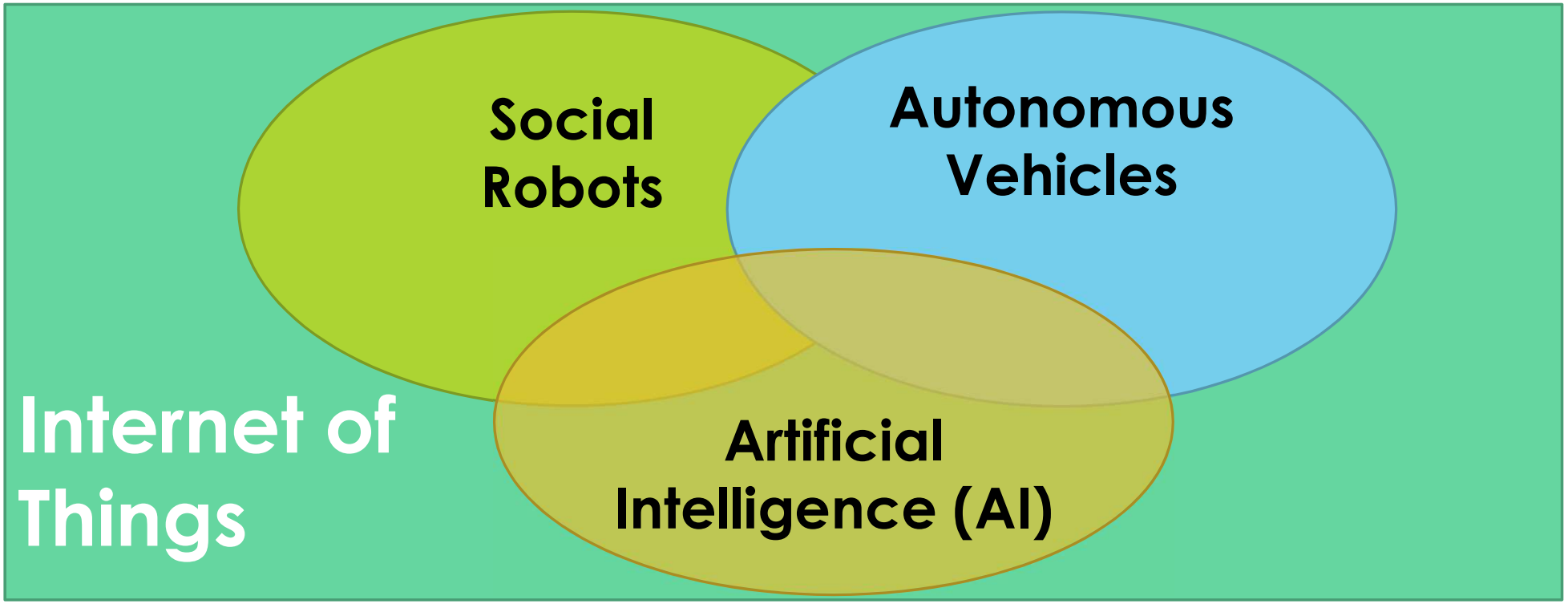
- **ERA Chair project funded under FP7 Pilot (2014-2019)**
  - Contributes to H2020 pillar "Spreading Excellence and Widening Participation" expected to close the research and innovation gap in the EU
- **Realisation of full potential of the Univ. of Žilina and its region in the field of Intelligent Transport Systems (ITS)**
- **ERAdiate impacts beyond Research and Innovation**
  - Internationalisation,
  - Fostering Inter- Trans- disciplinarity
  - Institutional and structural changes
  - Regional impact by involving public and private actors in ITS initiatives and projects

http://www.erachair.uniza.sk

About the H2020 project "MoTiV"
(Coordinator: University of Žilina, Slovakia)

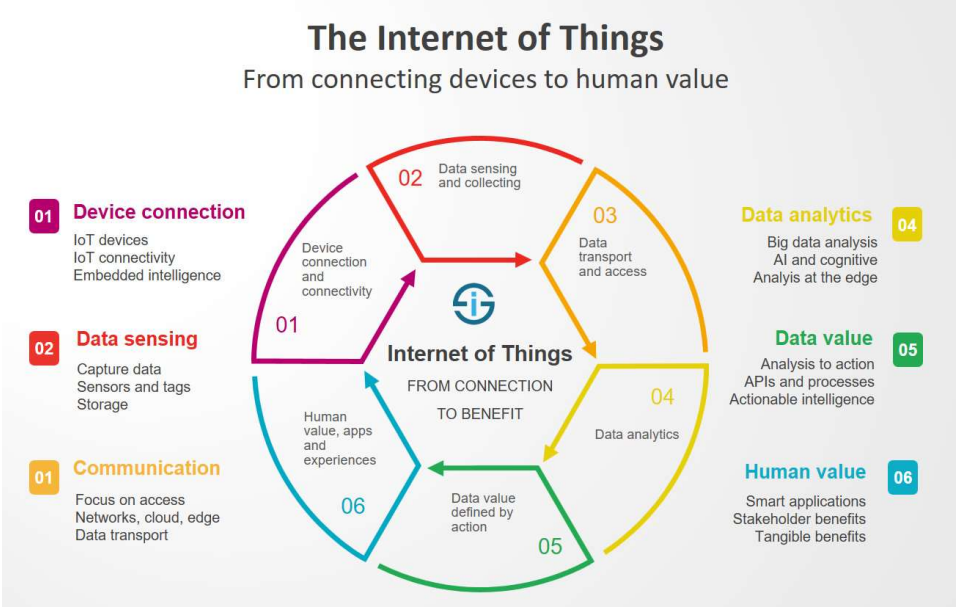
- **Mobility and Time Value (MoTiV): Research & Innovation Action acquired within the ERAdiate project**
  - Addresses topic of changing value of travel time in transport and mobility contexts
  - Consortium: 7 partners (3 academic, 3 companies, 1 end-user European-wide association)
  - Project duration: 1/1/2017 – 30/4/2020 (30 months)
  - A UNIZA success story: currently, MoTiV is the only H2020 RIA project coordinated by an academic institution in Slovakia
  - www.motivproject.eu

Context


Social Robots
Autonomous Vehicles
Artificial Intelligence (AI)
Internet of Things

Internet of Things (IoT) and the emerging "data-centric world"

- **Collection and processing of personal data** (and other types of data), a key IoT enabler and asset
- Aim is to deliver "human value", but success depends on how **data protection** and **security** issues will be addressed
  1. GPDR in Europe as legislative enhancement of the current framework
  2. Security and cybersecurity challenges
- What are the **implications for AI-based technologies and services**?



Legal framework in the EU

1. **Directive 95/46/EC – The Data Protection Directive**
2. **Article 29 Data Protection Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things**
3. **Directive 2016/679 - General Data Protection Regulation (GDPR)**
4. **Guidelines (e.g. Article 29 Data Protection Working Party WP251on Automated individual decision-making and profiling for the purposes of Regulation 2016/679)**

IoT Data: GDPR requirements

- ***Security Breaches:*** organizations handling personal data will need to ensure that they are in a position to ***identify and deal with security breaches*** while also introducing a ***mandatory notification system*** in the event of any breaches of personal data.

- ***Storage:***
  - adjust or implement storage systems following **privacy-by-design** framework.
  - comply with access regulations and **data minimization principles** as well as providing **adequate cyber security and protection measures** such as encrypting data at every possible opportunity.
  - application to storage mapping will also ensure that **any application can be mapped to the physical storage it occupies** with data being identified as containing personal information.

IoT Data: GDPR requirements

- ***Children and Consent:*** acquire and demonstrate a subject's consent to their data being processed and specifies that consent cannot be presumed through a subject not challenging the use of their data.

- ***Subject Rights:***
  - The **right to data portability** gives subjects the right to access and reuse their personal data across multiple online services.
  - The **right to erasure** allows subjects the express right to be "forgotten", meaning subjects can request the removal or deletion of personal data where there is no specific reason for its continued processing or storage.
  - The **right to object to automated decision making** for use in scenarios when a potentially damaging decision could be made without human intervention.

GDPR and AI-based business models

- **GDPR and related guidelines (such as WP251) will have an enormous impact on AI-based technologies (including autonomous vehicles and social robots)**

- **Interpretation of the new EU legal framework on data privacy not obvious**
  - *data subjects' access and information rights and the requirement to provide "meaningful information about the logic involved" are difficult to comply with*
  - it expects data controllers to "*find simple ways to tell the data subject about the rationale behind, or the criteria relied in reaching the decision*". However, AI decision-making is often opaque as AI systems may not be able to indicate how a decision is reached
  - *while requiring human intervention may ameliorate data protection risks, it may also negate the intended benefits of using AI.*

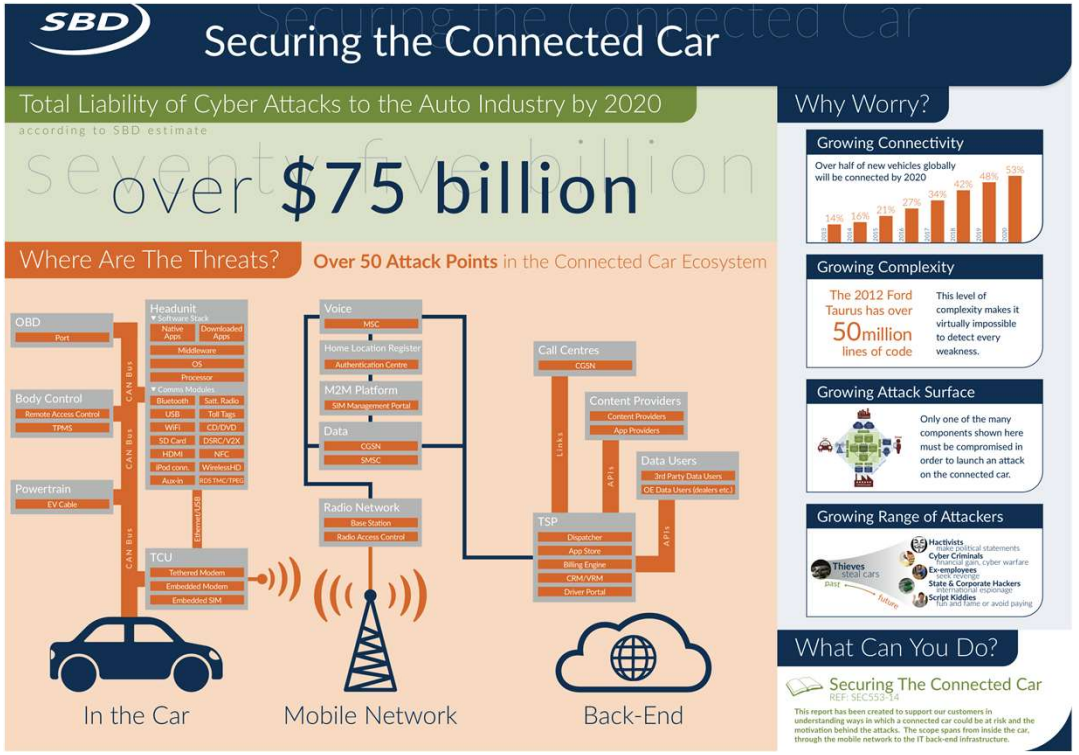
Data Privacy and Cybersecurity issues in IoT context (scenario: autonomous vehicles)

- **Cybersecurity is one of the GDPR requirements**
  - context of analysis: **autonomous vehicles**, an emerging and rapidly evolving IoT area in which AI plays a central role
  - In a connected environment, gaining access to autonomous vehicles likely to extend to other IoT devices
  - Considerations and recommendations may be extended to other IoT contexts (e.g. social robots)

- In the context of autonomous vehicles:
  - What **kind of data** is it collected?
  - **Who has access** to such data?
  - How could a **"malicious user"** use this data?

Addressing **cybersecurity in connected car environment**

- Priority for the automotive industry
- Massive investments
- Much uncertainty and complexity
- Technology advances much faster than legal framework
- If cybersecurity is not properly addressed, it could “kill” this emerging market (with strong and long-term effects on other IoT technologies and solutions)



Elon Musk and the Rhode Island Scenario

- In early 2017, **Elon Musk warned about the dangers of hackers** potentially taking control of thousands of driverless cars.
  - *"In principle, if someone was able to... hack all the autonomous Teslas, they could say - I mean just as a prank - they could say 'send them all to Rhode Island' - across the United States".*
  - *"And **that would be the end of Tesla**, and there would be a lot of angry people in Rhode Island"*

- **A possible solution:** a kill switch *"that no amount of software can override"* to *"ensure that you gain control of the vehicle and cut the link to the servers"*

Tesla can update its cars' software wirelessly, but what are the risks?

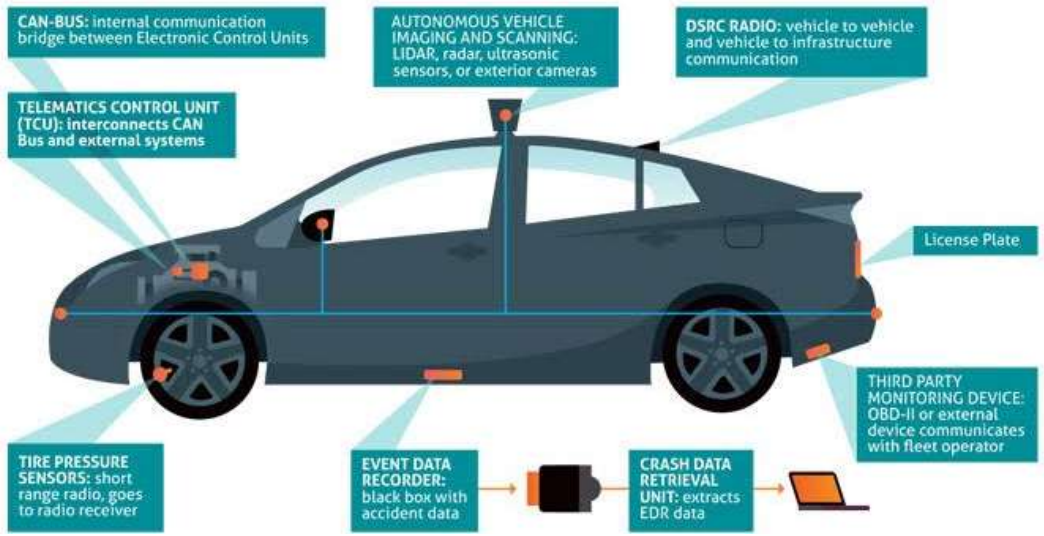
Can you be sure your self-driving car is taking you where you want to go?

IoT and Autonomous Vehicles: General security requirements

- **Resilience of attacks:** The system has to avoid single points of failure and should adjust itself to node failures
- **Data authentication:** Retrieved information must be authenticated
- **Access control:** Information providers must be able to implement access control schemes on their confidential data
- **Privacy:** Suitable measures should be implemented to protect nodes private information

IoT and Autonomous Vehicles: Data acquired

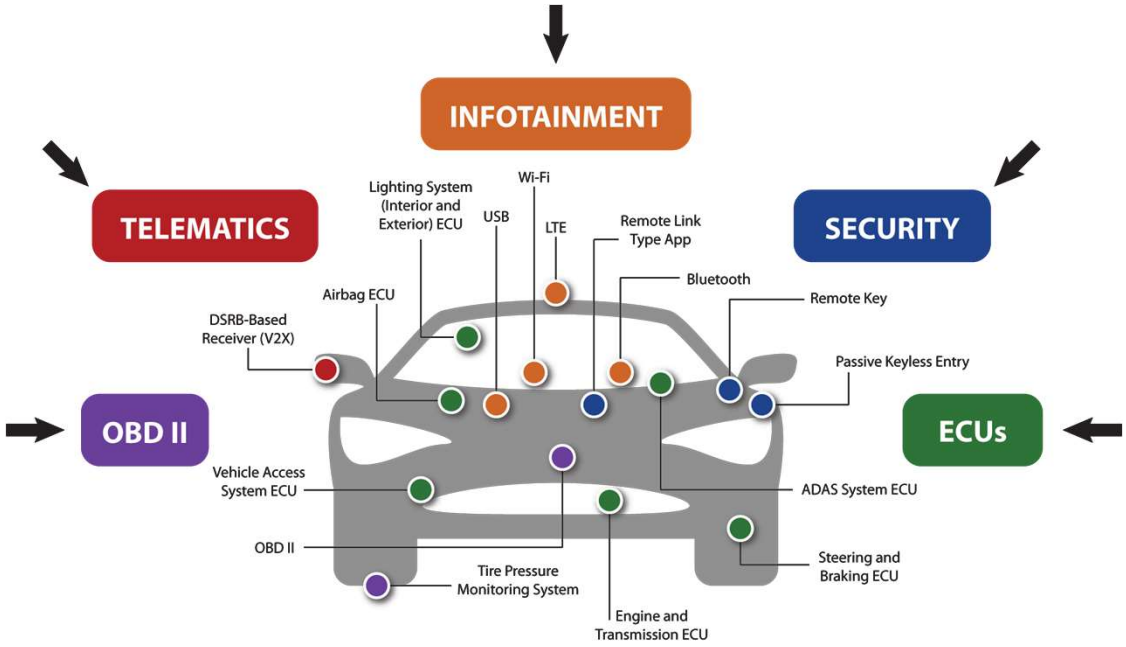
- **Geolocation:** GNSS, GSM, WiFi
- **External:** cameras, radars, lidars, sonars
- **Biometrics:** facial recognition, vital signs, voice samples
- **Behavioral:** driver's attention, speed, steering and braking habits, infotainment preferences…



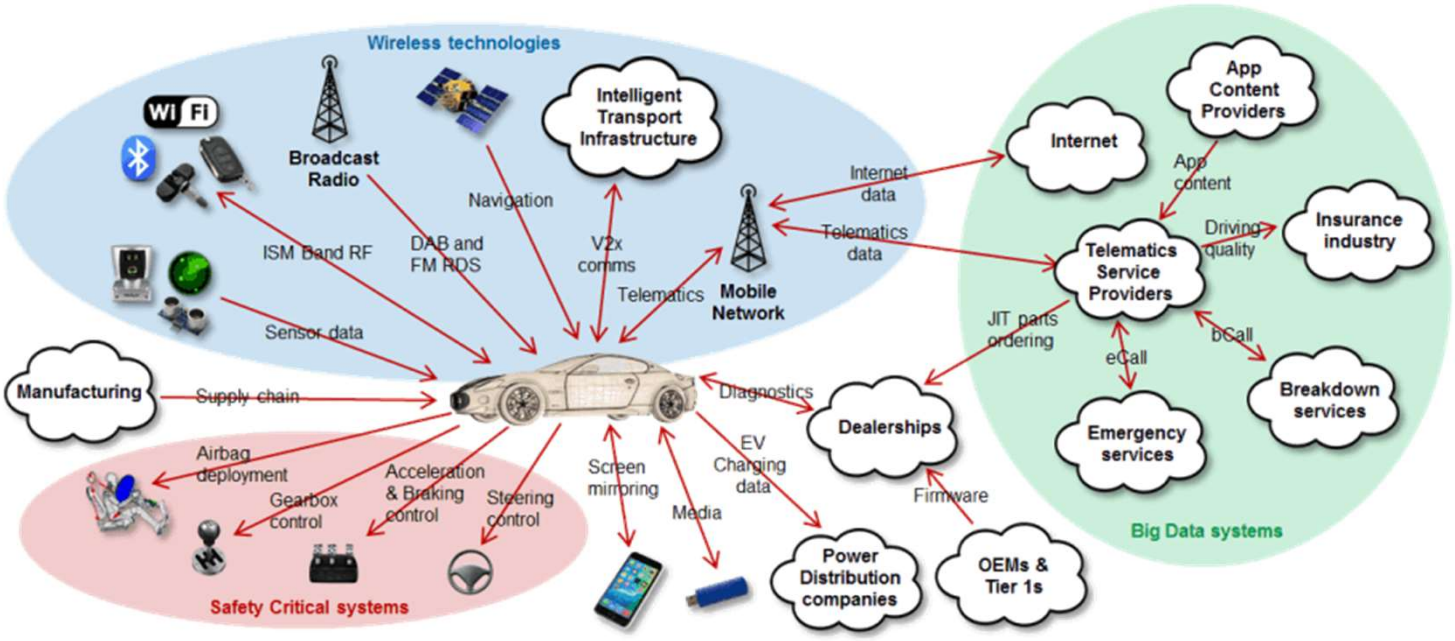
All data may be managed by an intelligent agent (e.g. virtual assistant) and shared within personal IoT eco-system and other connected services/platforms

Attack Surface Areas: What has to be considered?

- Rising number of always connected nodes becomes **more attractive for attackers**
- The attacker **tools are freely available and relatively easy to use** for anyone, even without deep IT security knowledge



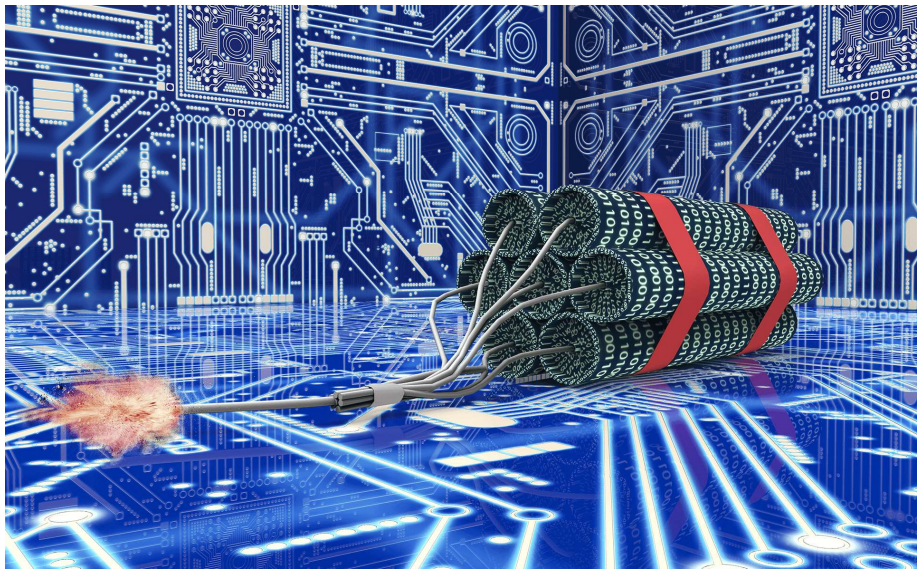
Attack Surface Areas: What has to be considered?



A **very complex environment**, with many players involved

Attack types and impacts

- **Threats to privacy**
  - Reconnaissance
  - Eavesdropping
- **Threats to control**
  - Man-in-the-middle
  - Radio interference
  - Injection
  - Replay
  - Byzantine
- **Threats to availability**
  - DoS or DDoS
  - Jamming
  - Collision
  - Wormhole
  - Node compromise

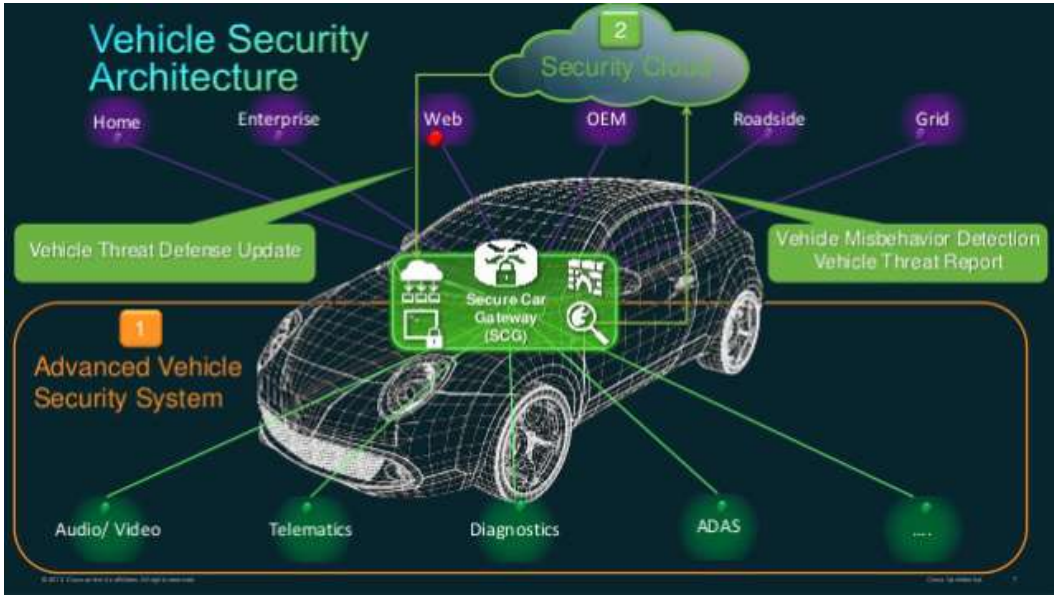


Testing the security aka **Penetration testing**

- **Exploiting vulnerabilities** present in the target system
- **Simulating attacks** using real-world techniques and tools in real-world environment
- Providing **mitigation recommendations**

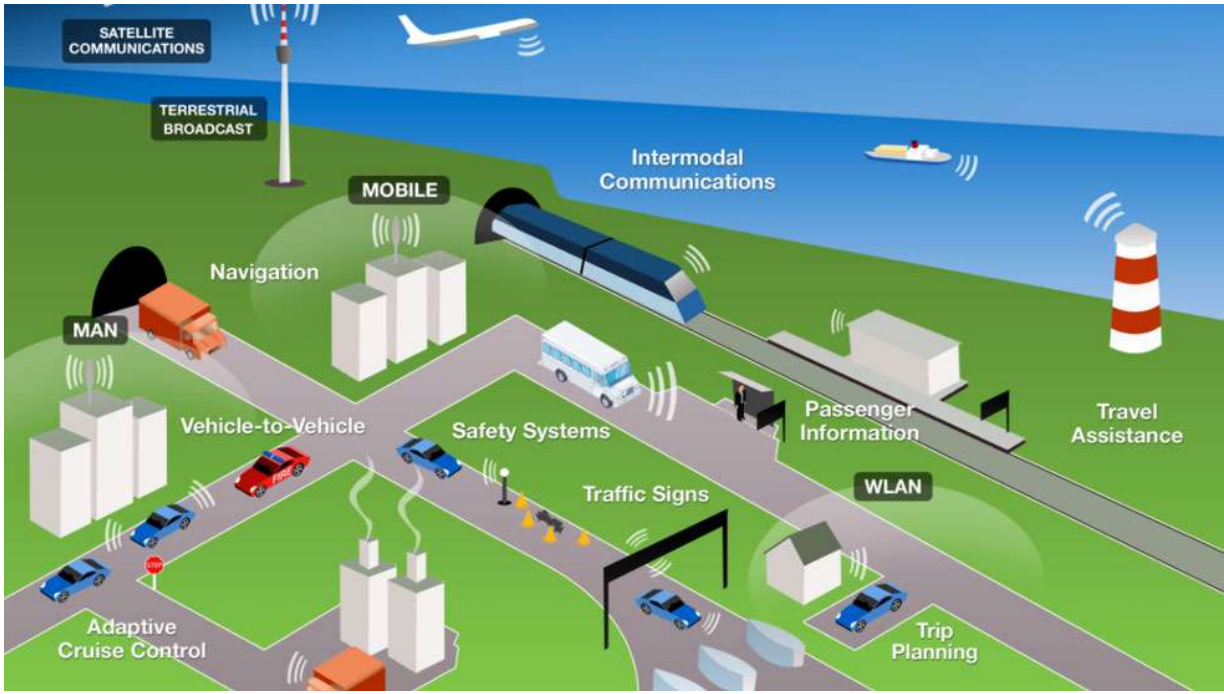
Countermeasures: What can be done?

- Intrusion detection/prevention systems & Firewalls
- Cryptography techniques (Public Key Infrastructure, PKI)
- Access control
- Secure wireless protocols
- Vulnerability & Update management
- …



Going further: Car2Car & Car2Infrastructure Communication Challenges

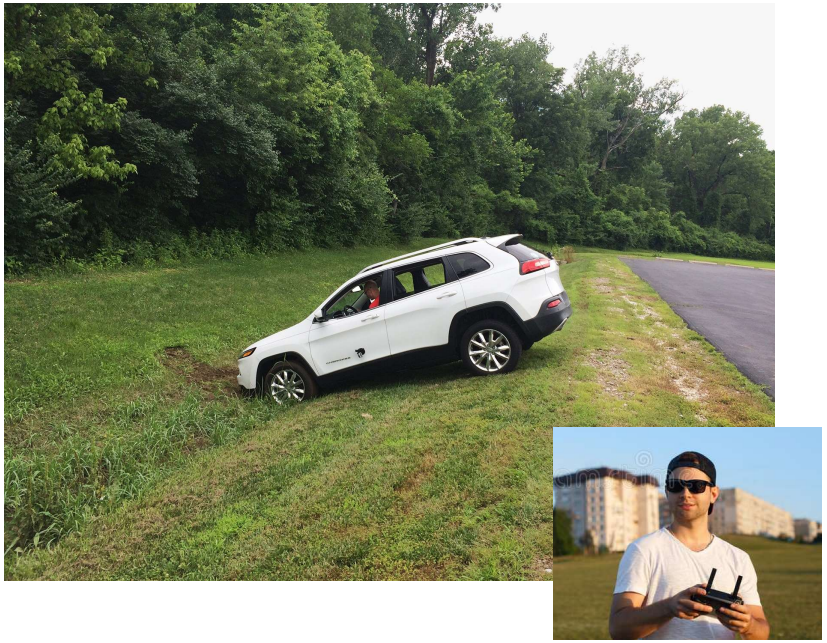
- The concept of Cooperative Intelligent Transport Systems (C-ITS)
- Creating network of potentially vulnerable data sources and sinks



It is starting to happen

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT (2015)

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (5:07)



IoT Data Privacy: are the GDPR and the current cybersecurity measures sufficient?

- In automated and connected car context, **cybersecurity risks are a serious threat**
  - GDPR requires to *adequately* address such risks
  - However, no IT (and IoT) system will ever be 100% safe

- What kind of **scenarios** could emerge in a future society in which **intelligent agents / social robots** are likely to co-exist with humans, and therefore **continuously collect and process (with advanced AI) personal data**?

Personal data, emotions and socially intelligent agents (aka social robots)

- **The "Her" scenario:** a man (Theodore) feeling strong **emotions and falling in love with an intelligent agent** (Samantha)?

- In the movie, Theodore **shares with** Samantha **everything, in every moment and everywhere**
  - The movie focuses on psychological and social aspects and does not address privacy or cybersecurity
  - However, a malicious user gaining access to the data collected by Samantha could produce severe harm (psychological and/or physical) against Theodore

Personal data, emotions and socially intelligent agents (aka social robots)

- **The "Real Humans" scenario:** hubots are part of society. Tv series characters feel strong **emotions and fall in love with hubots, who are also used as advanced sex-toys**

- Several interesting situations
  - **Humans develop an emotional bond with their hubot.** Replacing hubot (for an upgrade or because no longer functioning) not easy as replacing a smartphone.
  - **Hubots get infected with a computer virus** that compromises their functions (motor, linguistic etc)
    - **"First the soul, then the body":** synthetic body less important than synthetic soul (memories, experiences, personality). Can this be backed up and possibly exported to "clone"
  - **Legal framework not adequate to deal with emerging cases** (e.g. civil rights of a hubot – in tv series getting married to a human)



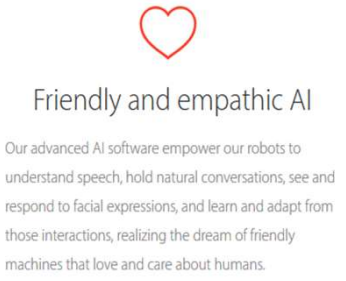


2017: Sophia, the first social robot declared as a citizen (of Saudi Arabia)

- "Real Human" scenario may not be just science-fiction: on 25 October 2017, **humanoid robot Sophia was recognized as a citizen** of Soudi Arabia during the "AI for Good Global Summit"
  - What kind of data is Sophia collecting? Who has access to it? For how long? How about consent requests?
  - If she's hacked, what could be the implications? Who would be responsible for any (psychological and/or physical) harm she could cause to others?
- **In EU, companies like Hanson Robotics must comply with regulations such as the General Data Protection Regulation (GDPR)**
  - Its application is even more challenging than in the connected and automated car context

Hanson Robotics

"we bring robots to life"



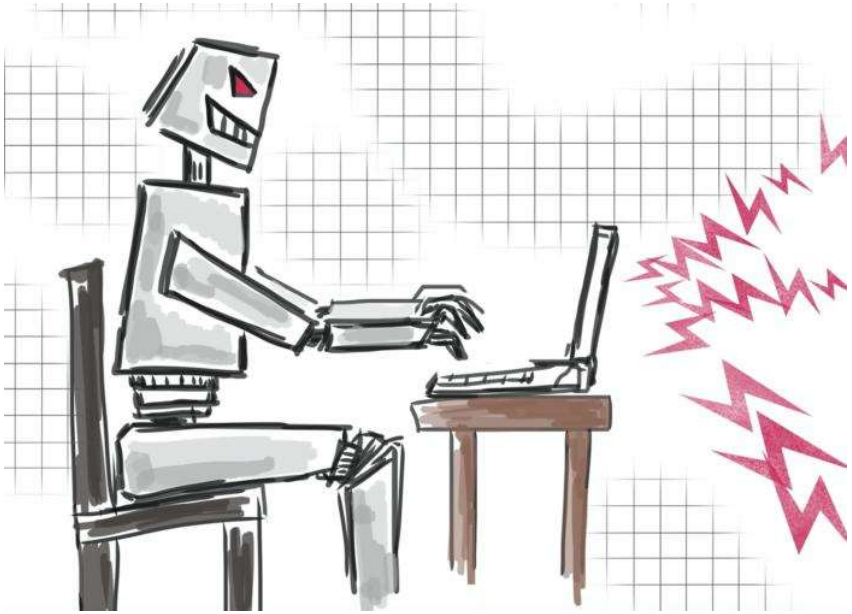
Final Considerations

Contradicting views

1. **A social robot (whatever intelligent) is still an IoT device**
   - Scope of action limited by legal framework (e.g. GDPR) and cyber-security measures (e.g. 'kill-switch')
   - At an emotional level, interactions shall be restricted to functional / rational ones (view of the robot as a "slave")

2. **A social robot is an intelligent agent, much more than a device**
   - Scope of action not limited: no "red line" defined for social robots (e.g. case of Sophia declared as a citizen)
   - What kind of rights / duties shall apply to social robots?
   - Emotional relationships with intelligent agents can be developed (view of the robot as a autonomous entity)

Final Considerations



How would we react if the IoT "malicious user" would the social robot itself?

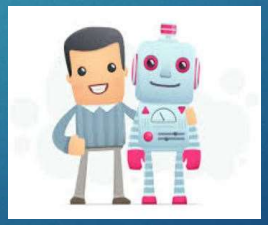
(or, even worse, a networked community of intelligent agents)

Thank you for your attention!

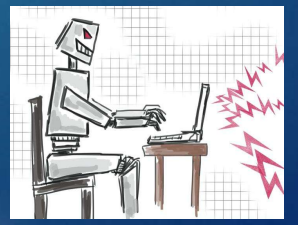
Question Time

ALSO VIA EMAIL:

MARTIN.HUDAK@ERACHAIR.UNIZA.SK



OR



?