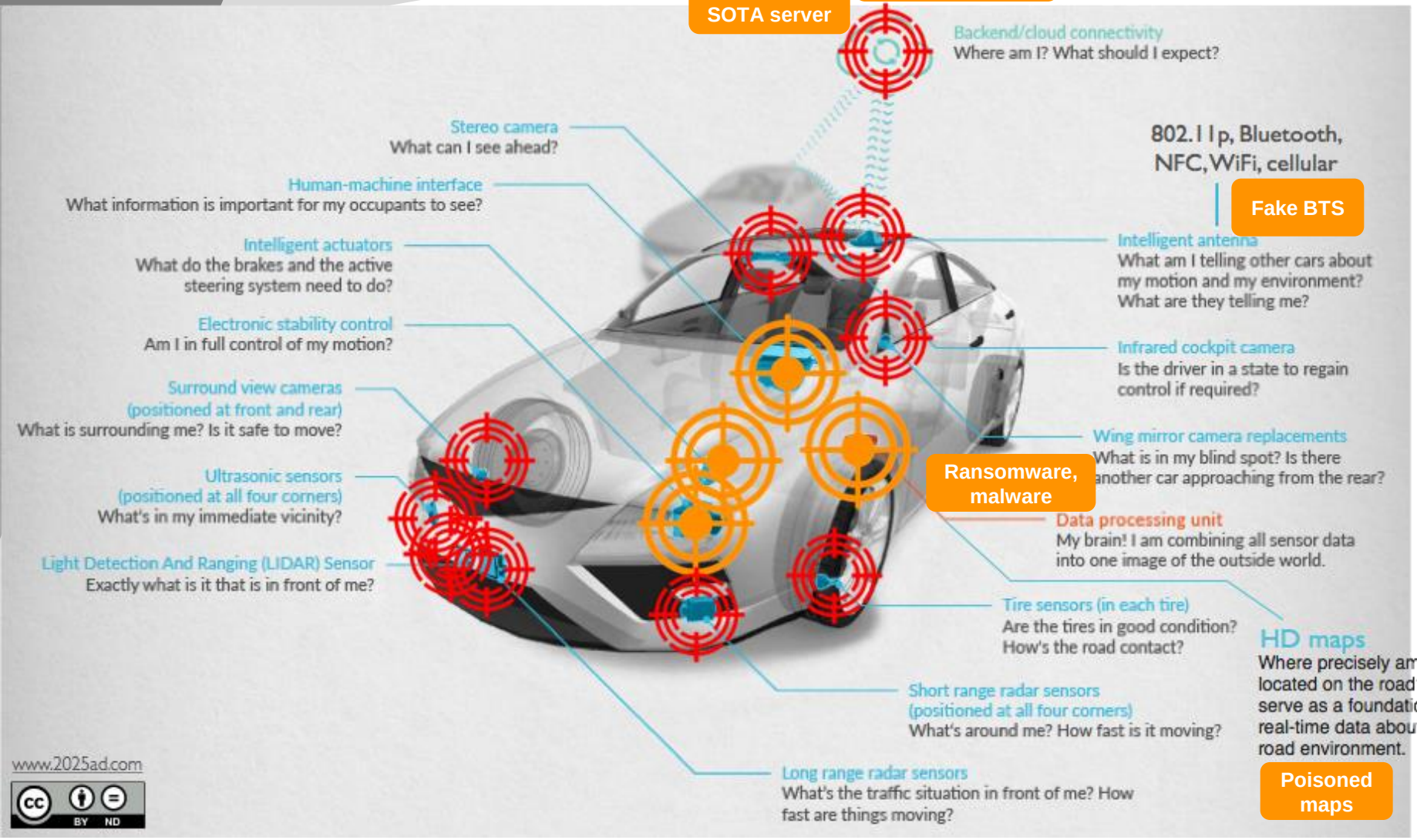
info security
STRATEGY | INSIGHT | TECHNOLOGY
BOSTON CONFERENCE | 06-07 DECEMBER 2016

SECURITY INNOVATION
EMBEDDED

Keeping up with Next-Generation of Cyber Risks:

Securing the Connected Car


Attacks on SOTA server
Compromised PKI components
Backend/cloud connectivity
Where am I? What should I expect?
802.11p, Bluetooth, NFC, WiFi, cellular
Fake BTS
Stereo camera
What can I see ahead?
Human-machine interface
What information is important for my occupants to see?
Intelligent actuators
What do the brakes and the active steering system need to do?
Electronic stability control
Am I in full control of my motion?
Surround view cameras (positioned at front and rear)
What is surrounding me? Is it safe to move?
Ultrasonic sensors (positioned at all four corners)
What's in my immediate vicinity?
Light Detection And Ranging (LIDAR) Sensor
Exactly what is it that is in front of me?
Intelligent antenna
What am I telling other cars about my motion and my environment? What are they telling me?
Infrared cockpit camera
Is the driver in a state to regain control if required?
Wing mirror camera replacements
What is in my blind spot? Is there another car approaching from the rear?
Ransomware, malware
Data processing unit
My brain! I am combining all sensor data into one image of the outside world.
Tire sensors (in each tire)
Are the tires in good condition? How's the road contact?
HD maps
Where precisely am I located on the road? Also serve as a foundation for real-time data about the road environment.
Short range radar sensors (positioned at all four corners)
What's around me? How fast is it moving?
Long range radar sensors
What's the traffic situation in front of me? How fast are things moving?
Poisoned maps
www.2025ad.com

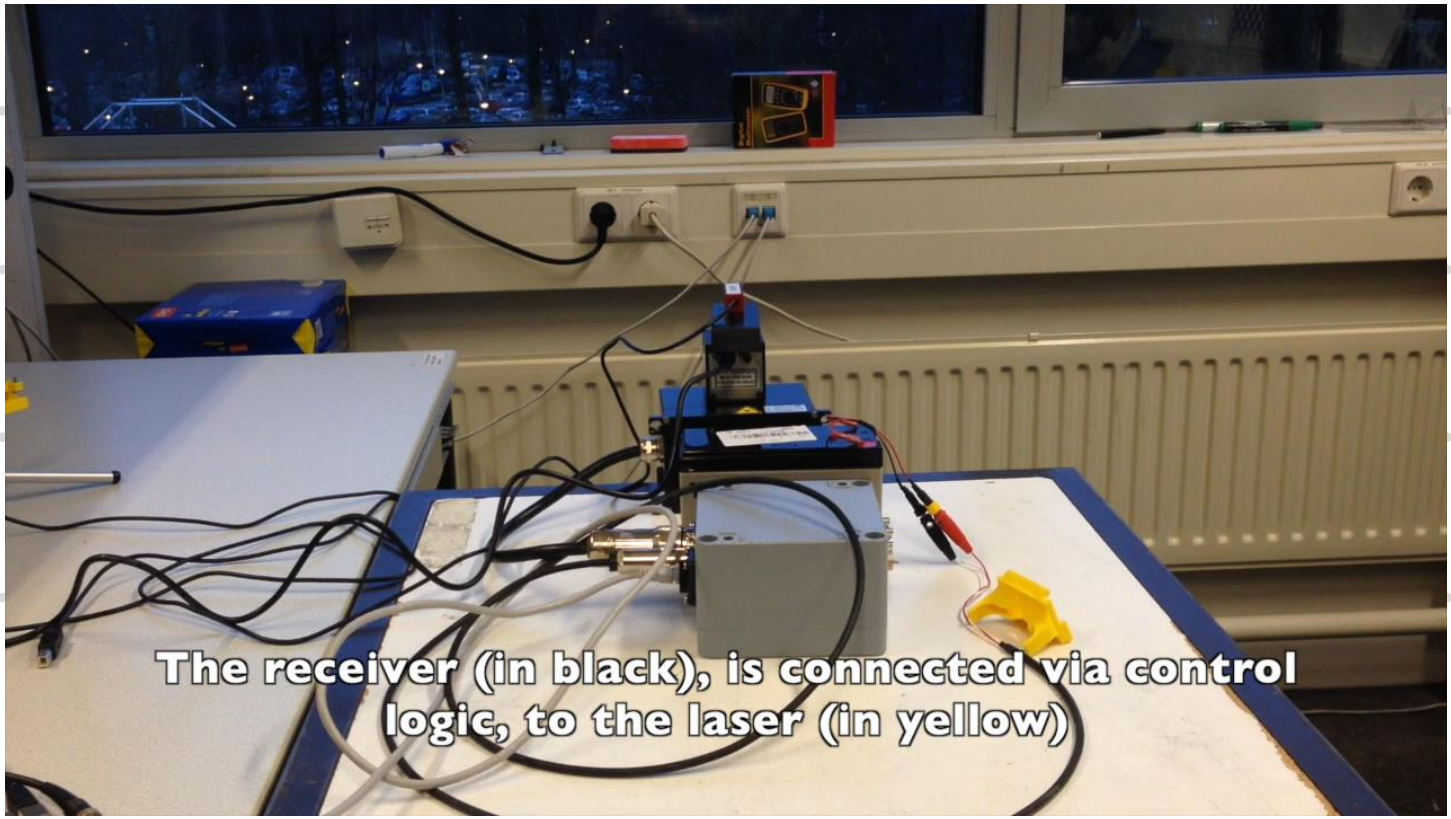
Current automotive industry efforts

- Firewall
- Bus separation
- Authentication on CAN-FD
- Intrusion Prevention System
- Software / Firmware Over-The-Air Update
- Participation to the Auto-ISAC

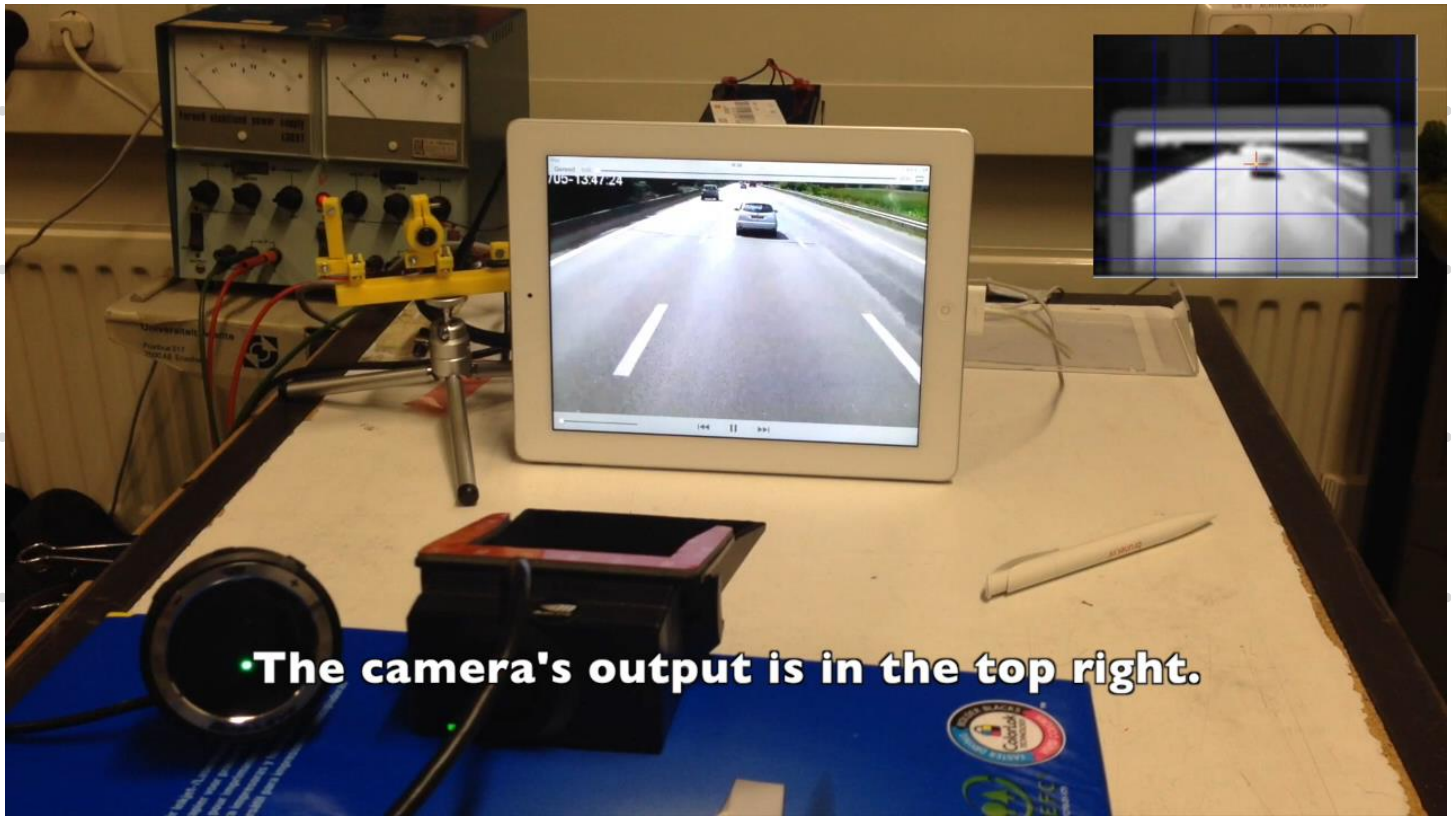
Why is the future potentially more prone to security threats?

Spoofing ultrasonic sensors

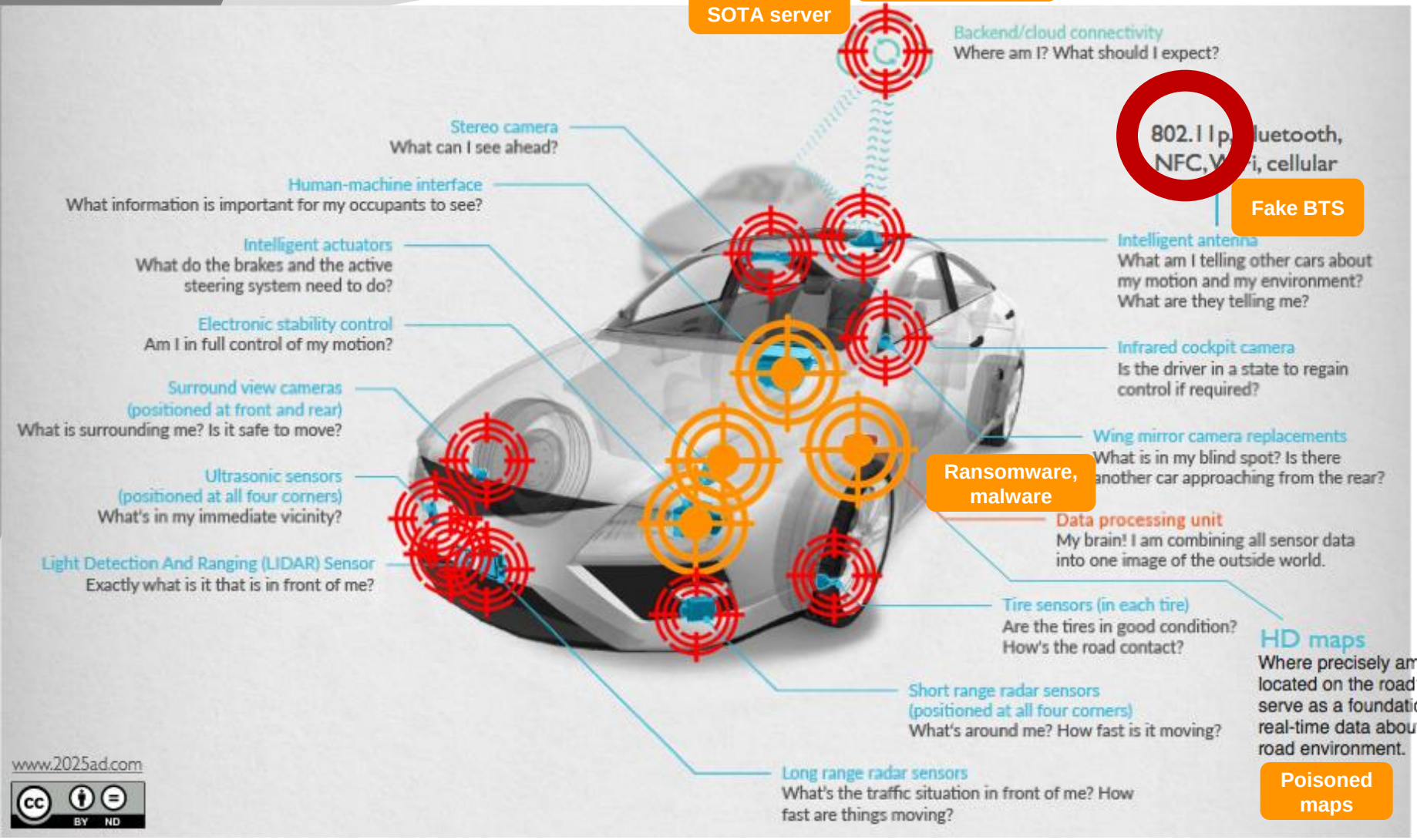
Spoofing RADAR



Spoofing LIDAR



Blinding camera


Attacks on SOTA server
Compromised PKI components
Backend/cloud connectivity
Where am I? What should I expect?
802.11p, Bluetooth, NFC, Wi-Fi, cellular
Fake BTS
Stereo camera
What can I see ahead?
Human-machine interface
What information is important for my occupants to see?
Intelligent actuators
What do the brakes and the active steering system need to do?
Electronic stability control
Am I in full control of my motion?
Surround view cameras (positioned at front and rear)
What is surrounding me? Is it safe to move?
Ultrasonic sensors (positioned at all four corners)
What's in my immediate vicinity?
Light Detection And Ranging (LIDAR) Sensor
Exactly what is it that is in front of me?
Intelligent antenna
What am I telling other cars about my motion and my environment? What are they telling me?
Infrared cockpit camera
Is the driver in a state to regain control if required?
Wing mirror camera replacements
What is in my blind spot? Is there another car approaching from the rear?
Ransomware, malware
Data processing unit
My brain! I am combining all sensor data into one image of the outside world.
Tire sensors (in each tire)
Are the tires in good condition? How's the road contact?
HD maps
Where precisely am I located on the road? Also serve as a foundation for real-time data about the road environment.
Poisoned maps
Short range radar sensors (positioned at all four corners)
What's around me? How fast is it moving?
Long range radar sensors
What's the traffic situation in front of me? How fast are things moving?
www.2025ad.com

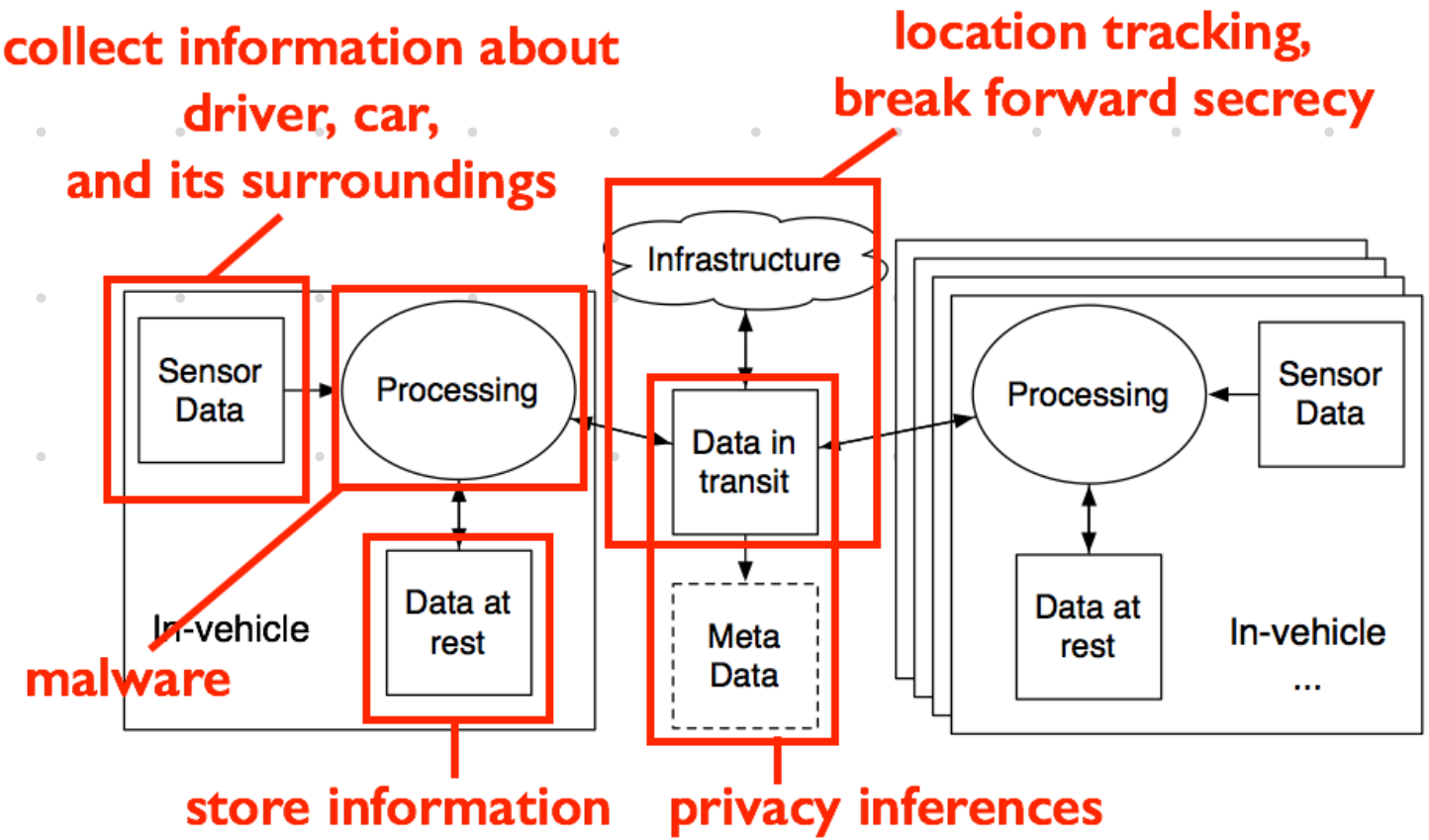
V2X Security & Privacy Controls

- Authentication using digital signature
- Pseudonymity
- Revocation
- Use of HSM / TPM
- Misbehavior Detection
- PKI (SCMS): security and privacy by design

V2X Security & Privacy Controls:
Can we do better?

- Authentication: quantum-safe cryptography
- Pseudonymity: pseudonym change strategies
- Revocation
- Use of HSM / TPM
- Misbehavior Detection: local and global algorithms
- PKI (SCMS): consider malicious components

Potential Privacy Violations



Bigger Privacy Issues in AV?

- AV data are rich (richer than CV): sensors data, driver information?
- AV data are stored in-vehicle and in the cloud
- Richer data are shared with neighboring AVs because this isn't only a warning system anymore
- AV data will be used for forensics/insurance
- Cloud can send command to the AV to control it (fleet of autonomous vehicles that could be tele-operated)

What can we do?

- Mitigations
- Risk assessment
- Collaboration
  - Common lab for cybersecurity testing
  - Cybersecurity rating
  - Hire security experts

Composition problems

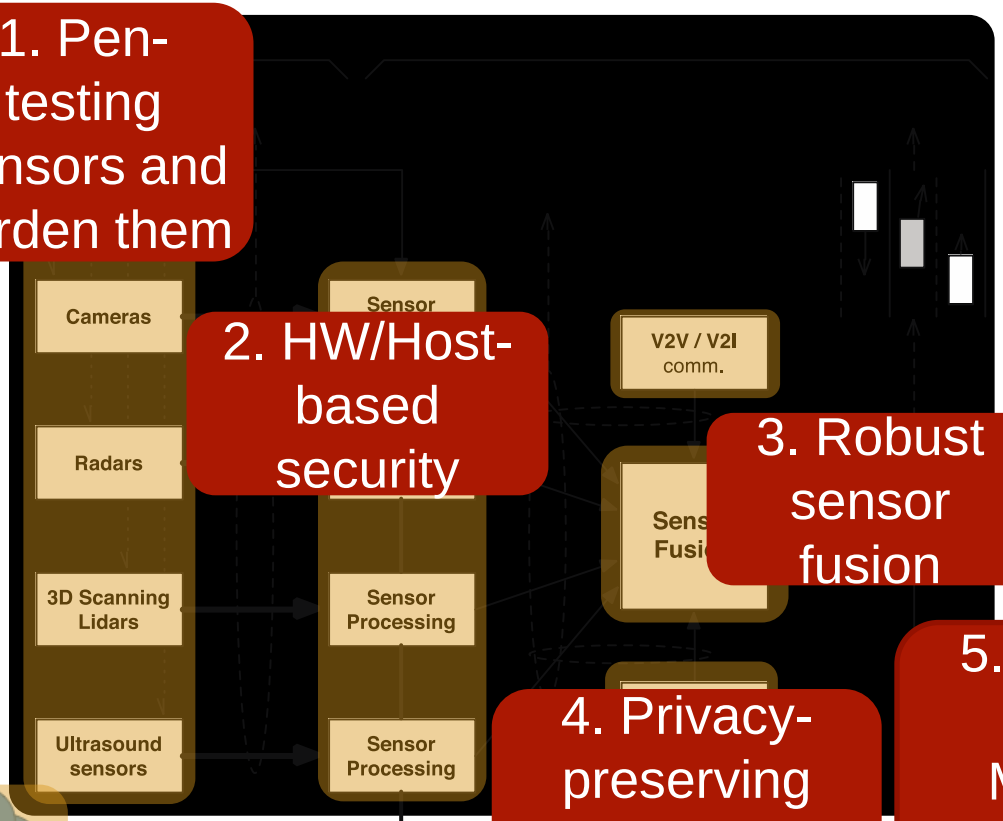
1. Pen-testing sensors and harden them

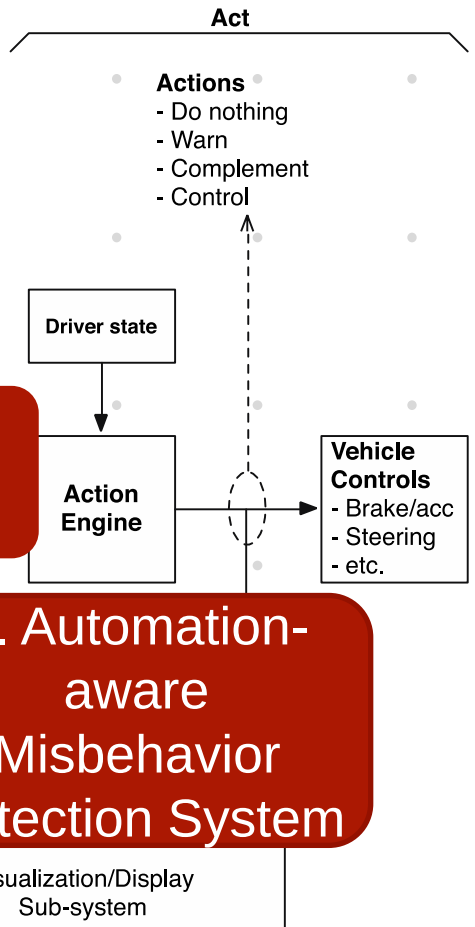
2. HW/Host-based security

3. Robust sensor fusion

4. Privacy-preserving data sharing protocol

5. Automation-aware Misbehavior Detection System





Interoperation issues between safety, security and privacy

Takeaways

1. Connected Vehicle is a complex system that requires Security and Privacy by design because these have fundamental implications.
2. Move from “Security = cost” mindset to “Security = Safety + User Satisfaction”
3. Foster collaboration by building common cybersecurity lab
4. Still significant open challenges!