Cybersecurity Engineering and Assurance for Connected and Automated Vehicles

Paul Wooderson

13 November 2018

Vehicle cybersecurity concerns

Privacy – vehicle as a data hub

Used connected cars need disconi

National Cyber Security Centre
a part of GCHQ

Once upon a time you sold your car, handed over the k
pocketed the cash or bought a new car and thought no
connected world – you may have just sold a computer

As of late 2017 there were around 9 million internet-connected cars on UK roads. Most new cars have features that allow the owner to interact with the vehicle, even when nowhere near it. This varies from the ability to set climate control, through to uploading sat nav destination details and more. This information is then stored in the online account associated with the car.

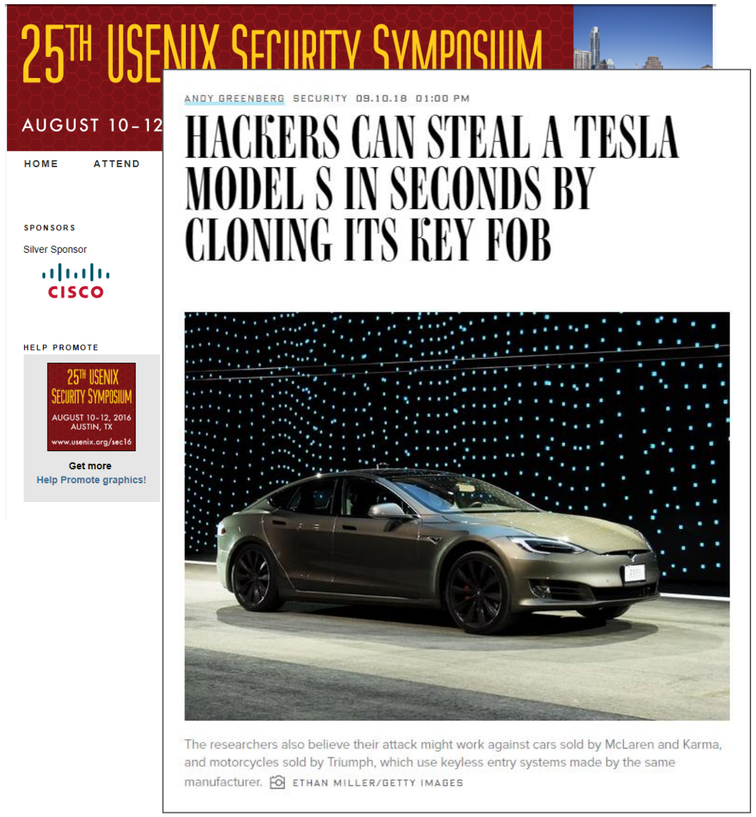
This data is not the only personal information that remains with the car. For instance, phones that have been paired with the car should also be unpaired when the car is sold.

When selling an old phone or device most people would ensure that any personal data on it was completely wiped. The same principle applies when an internet-connected car is sold; it is generally the seller's responsibility to disable the online account that they used with that car.

Many car manufact
customers may not
When the car is the
other data without t

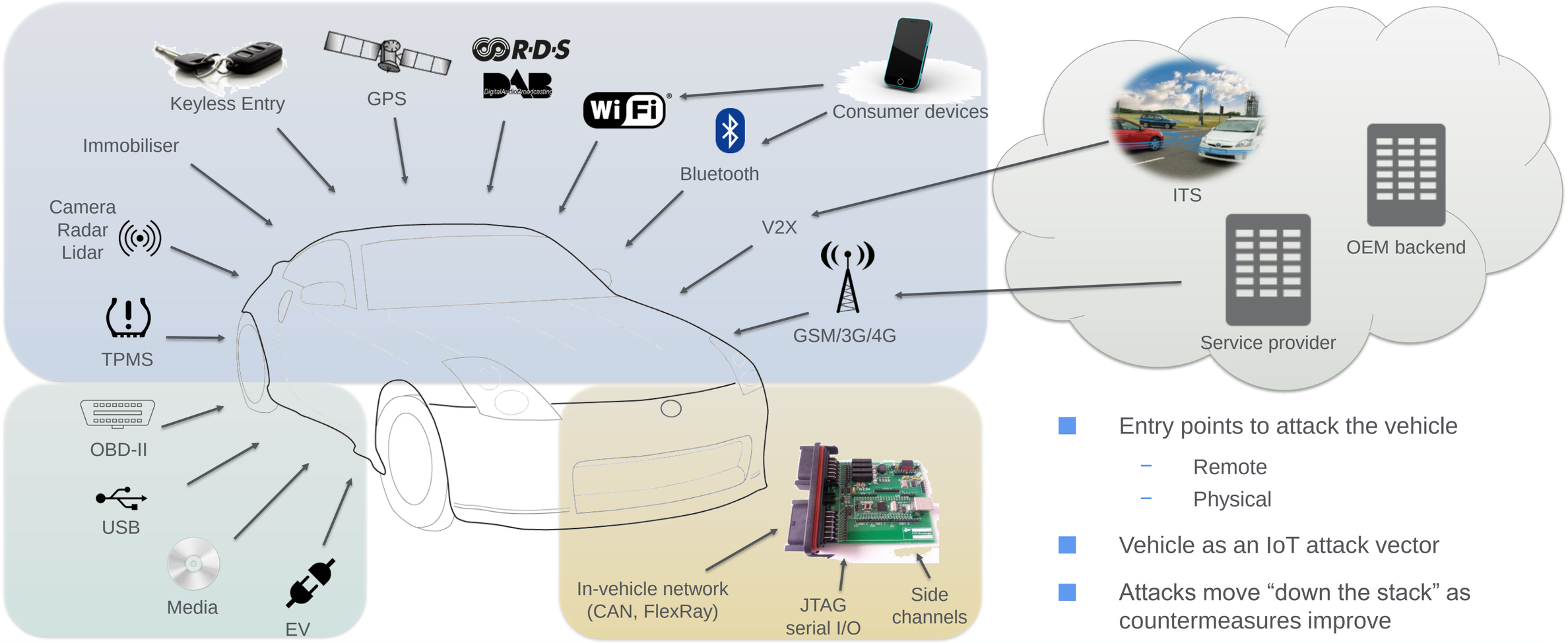
The key message is
delete all personal
already seen as a k
devices should alsc

Theft – physical → cybersecurity



Safety - impacts of security failures now include injury or death

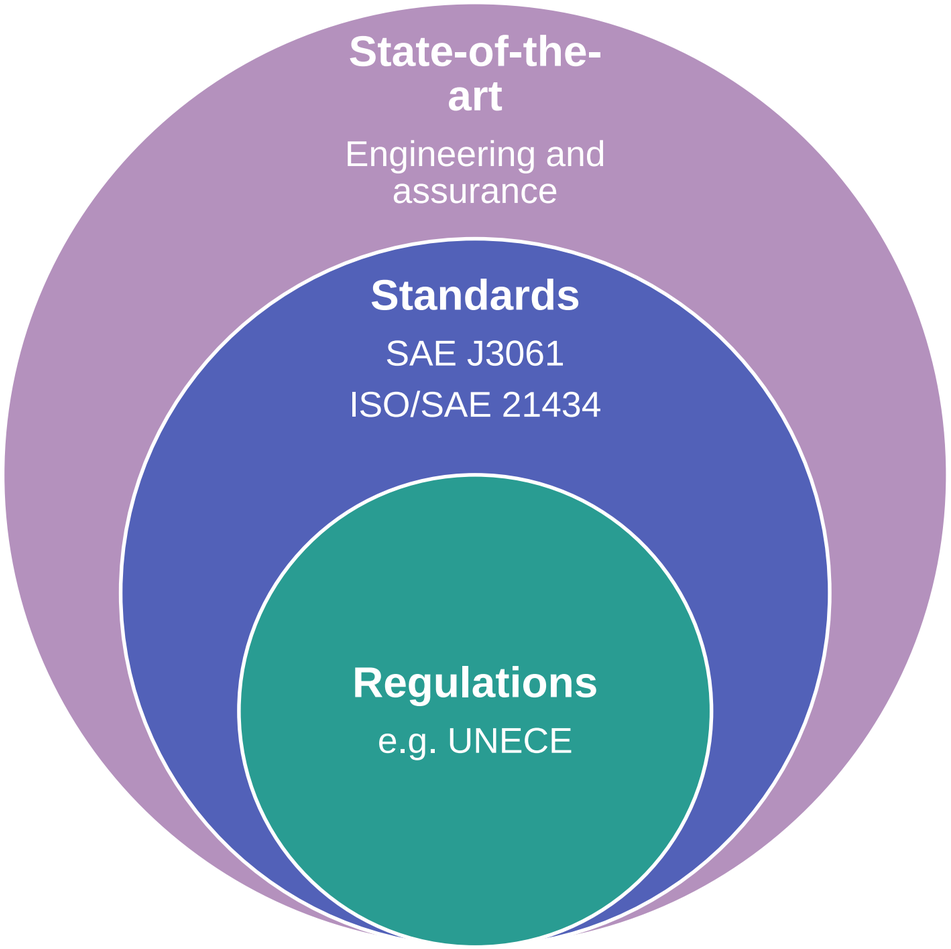
The vehicle attack surface



- Entry points to attack the vehicle
  - Remote
  - Physical
- Vehicle as an IoT attack vector
- Attacks move “down the stack” as countermeasures improve

Standards, regulations and state-of-the-art

- **Regulations** mandate the **minimum acceptable** requirements e.g. for type approval
- **Standards** define common requirements based on **industry accepted** best practice
- How can we "**raise the bar**" to:
  - Ensure consumers are able to trust connected and autonomous vehicle technology in the long term
  - React more effectively to the dynamic threat landscape
  - Address cybersecurity in the context of other related risk-based disciplines

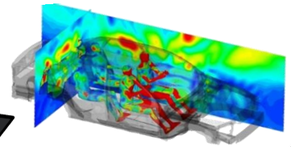


Risk driven engineering approach

PROACTIVE ENGINEERING

Development Lifecycles Based on
Risk Driven Systems Engineering
(ISO 26262, ISO/PAS 21448, SAE J3061, ISO/SAE 21434)

Requirements, Hazard, Threat & Risk Analysis



Early Design Verification

- Safety
- Security
- Functionality
- Reliability

Verification, validation and assessment

- ☑ Training and seminars
- ☑ Process development
- ☑ Engineering support
- ☑ Testing and validation
- ☑ Assessment and assurance

REACTIVE ENGINEERING

What is assurance?

- Assurance means “confidence” rather than “guarantee”

- How confident can we be that:
  - The **design** of the product has taken security into account and addresses the relevant threats
  - The **implementation** of the product achieves the expected level of security
  - Appropriate processes are in place to respond to incidents during the **lifetime** and are effective

- Assurance is more than just testing, it is **built up** based on a combination of activities throughout the lifecycle

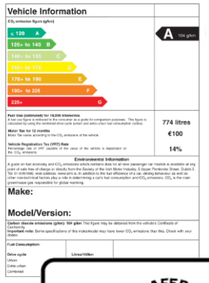
Who needs assurance for connected autonomous vehicles

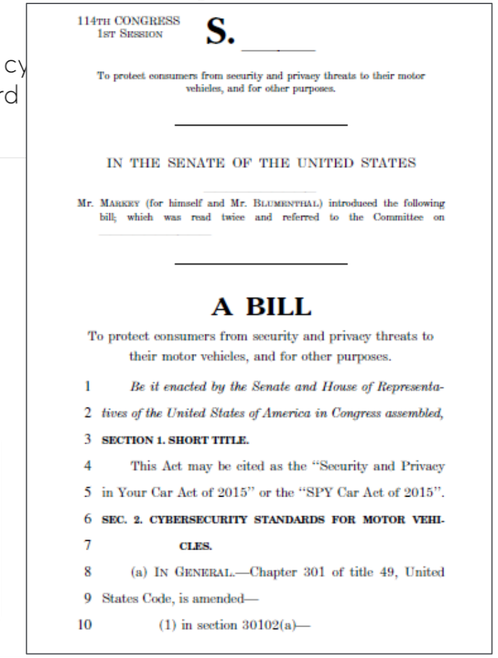
- **Product vendors** for their own products and for the components supplied by their supply chain
- **Consumers** need to have confidence that their vehicle is safe
- **Insurers** need to understand how to price cybersecurity risk
- **Governments** need to understand risks to critical infrastructure

Consumer Reports to Begin Evaluating Products, Services for Privacy and Data Security

CR partners with other cy
source industry standard

By Consumer Reports
March 06, 2017





114TH CONGRESS
1ST SESSION

S. _____

To protect consumers from security and privacy threats to their motor vehicles, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. MARKEY (for himself and Mr. BLUMENTHAL) introduced the following bill; which was read twice and referred to the Committee on

A BILL

To protect consumers from security and privacy threats to their motor vehicles, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Security and Privacy in Your Car Act of 2015" or the "SPY Car Act of 2015".

SEC. 2. CYBERSECURITY STANDARDS FOR MOTOR VEHICLES.

(a) IN GENERAL.—Chapter 301 of title 49, United States Code, is amended—

(1) in section 30102(a)—

*"**Cyber is something customers are making purchasing decisions on**," he said, adding that the customer's notion of a particular company's cybersecurity proficiency is likely to become like many other competitive metrics when it comes to winning a spot on a buyer's consideration list.*
(Jeff Massimilla, GM, http://articles.sae.org/15549/)

Automotive Cybersecurity Through Assurance

- 5StarS is a consortium partnering HORIBA MIRA, Ricardo, Roke, Thatcham Research and Axillium Research
- “Automotive Cybersecurity Through Assurance” is a collaborative research project funded by **InnovateUK** to address cybersecurity for connected and autonomous vehicles
- The project will
  - Research and develop an innovative assurance methodology to assure that vehicles and their components have been designed and tested to the relevant cybersecurity standards
  - Research and develop a consumer and insurer oriented rating framework, analogous to existing EuroNCAP type ratings for vehicle safety
  - Align with relevant existing and emerging standards and regulations
- The project will address the challenge of establishing meaningful ways of providing cybersecurity assurance to consumers

www.5starsproject.com

Automotive Cybersecurity Through Assurance

- Leveraging best practices from other sectors, to deliver cybersecurity assured connected and autonomous vehicles more quickly than through legislation/standards alone

Contact Details

Paul Wooderson
MEng CEng MIET

Cybersecurity Principal Engineer & Team Leader

Direct T: +44 (0)24 7635 5244
Mobile T: +44 (0)7731 010066
E: paul.wooderson@horiba-mira.com

HORIBA MIRA Ltd.
Watling Street,
Nuneaton, Warwickshire,
CV10 0TU, UK

T: +44 (0)24 7635 5000
F: +44 (0)24 7635 8000

www.horiba-mira.com