Government
Office for Science

Foresight Future of Mobility project

Security Roundtable

2 October 2017, 0930 to 1100, 1 Victoria Street
Chaired by Professor Chris Whitty (Chief Scientific Adviser, Department for Transport)

This is an abridged summary of the roundtable, and in the spirit of free and open discussion, comments have not been attributed to specific attendees.

The roundtable was structured around three main questions regarding the security of transport systems:

- Will future technologies enable us to increase the safety and security of the transport system?
- Will future modes of transport (Mobility as a Service (MaaS) for example) present unique security challenges?
- How much of a role will government play in convincing the public that new transport technologies are safe and secure?

Key Points

- Unmanned Aerial Vehicles (UAV) and securing the wider airport campus are emerging security challenges in aviation.
- Road has a narrow window for security checks, and Connected and Autonomous Vehicles (CAV) present both security opportunities and vulnerabilities, being complex systems of systems with many stakeholders.
- Designing-in infrastructure security is difficult due to its long life, and integration of CAVs to smart infrastructure could provide opportunities for enhanced security monitoring.
- Big data and machine learning will allow anomalous patterns and unusual behaviour to be detected, though government should explain any data capture taking place, and how it benefits the public.

Aviation

Safety or Security?

- Mustn’t lump safety and security together – this is about security.
- Primarily about Counter-Terrorism (CT), so we need to think about intent and capability of attackers.

- Innovation depends on people knowing and understanding what could be deployed, and the risks associated with deploying a particular technology.

Aviation security challenges

- Threats change frequently, from versatile and fast moving enemies.
- Use of Unmanned Aerial Vehicles (UAVs) (‘drones’) is emerging as a threat, including against aviation.
- Drones will become increasingly common and capable, flying faster and further for longer, and could be used maliciously.
- How do we keep the airport campus safe, whilst ensuring smooth running of the infrastructure?

Integration with other transport modes

- Multi-ports with merged rail and air connections were suggested as an idea for the future, along with further integration of transport modes.
- Using passenger’s time on the train to undertake security checks (or other relevant processes, such as immigration clearance) was suggested.
- Would this transfer airline security requirements to other sectors?
- Who would pay for shifting checks in this way?

Maritime

The maritime sector faces different threats to other sectors

- Securing maritime freight (as opposed to passengers) is an important issue that differs from other sectors.
- Sector has reported issues with the surveillance of communication systems and spoofing of navigation systems posing a risk.
- Alternative fuels are more of a technology issue for maritime transport.

Rail

Wider deployment of technology could make railways more secure

- It is theoretically possible to remotely control a train via cyber-attack, although this has not been currently been demonstrated in practice.
- Who will pay for the deployment of security technology; how will you deploy it; how much will the public accept the technology being used; and how invasive can the security measures be?

Road

Road is a very different environment in which to implement security

- Cars are designed for anyone to get in and use at any time, with a focus historically on occupant safety.
- The advent of Autonomous Vehicles (AV) represents a significant change in automotive technologies, so there is an opportunity for a clean slate.
- Introducing identity checks would be a big technical ask, and likely spark a debate on privacy.

AVs versus Connected Vehicles

- Increasing levels of connectivity of vehicles gives a greater attack surface, with opportunities for remote hacking and control.
- Connected vehicles could be also face having the messages sent to them spoofed or jammed, creating a denial of service attack, or nuisance problems for the operator.
- If an attack enabled the taking control of vehicles, this could represent a threat to life.
- Manufacturers are working upstream on preventing attacks, working with suppliers on cryptography, authentication of components and code, gateways; mid-stream looking at integration of systems (such as apps) linking to other transport systems; and downstream, looking at the response to security events.

Increasing technology in road vehicles

- Connected and Autonomous Vehicles (CAV) will be highly complex system of systems.
- These will all require updates and patches, as customers will expect upgraded functionality and bug fixes.
- Huge amounts of data will need to be exchanged across sub-systems and through systems.
- Securing all sub-systems means ensuring the integrity of the supply chain.
- Will also need to be wary of backdoors introduced by legacy software or connected devices such as dongles.
- There are numerous intermeshed stakeholders – who will assume responsibility for security of the overall system?

The future for road vehicles

- Vehicles are becoming more complex, with a lot more assets to manage, and connected on-board safety and entertainment systems.
- Possible innovations could see driver and vehicle authentication systems integrated into the vehicle.
- Other innovative measures could help stop pedestrians being hit by vehicles and other types of vehicle accidents, prevent drunk/drug driving, and curb excessive speed.

Infrastructure
Securing transport infrastructure is also a key consideration

- The design life of infrastructure can be up to 120 years, and it’s difficult to design-in security this far into the future.
- Many aspects of the infrastructure have shorter lifespans, and can be upgraded or changed to improve security.

- Road assets and infrastructure might be vulnerable to disruption if they are controlled electronically.
- To improve transport efficiency and safety there is a desire to integrate CAVs to ’smart’ infrastructure, and there could be opportunities to enhance the security of both.

Data sharing for security

Can data or intelligence on threats and vulnerabilities be shared?

- The Cyber Security Information Sharing Partnership (CiSP)[1] is a useful model where information can be shared in a trusted environment.
- Where it is occurring, the benefits of any data capture needs to be explained to the general public, and the organisation undertaking it needs to ensure that it is beneficial to the general public, and does not impinge unnecessarily on their privacy.
- Highlight the balance between sharing data and the benefits the customer gets back, and make the case for security.
- Big data and machine learning provide opportunities for security by detecting anomalous patterns and unusual behaviour.

The government’s role in transport security

What could government do more (or less) to ensure transport security?

- Government can support or stifle innovation, but its support for CAV trials is encouraging.
- Need to have clarity on who is legally liable for CAVs, which will require legislation – the Automated and Electric Vehicle Bill[2] currently before Parliament will address these issues. Liabilities around Mobility as a Service (MaaS) also need clarification.
- The industry needs help in certifying CAVs, and ensuring that people can put their trust in vehicle systems.
- The government could facilitate greater public-private information sharing on the likely threats, so industry can design better responses.
- Government could consider drafting guidelines for the security of multimodal transport, such as those set out for CAV.
- Government also has a role in joining up different modes of transport, due to its convening power.

[1] www.ncsc.gov.uk/cisp

[2] https://services.parliament.uk/bills/2017-19/automatedandelectricvehicles.html

We would like to thank the following organisations for participating:

Atkins, the Civil Aviation Authority, Ford, Heathrow, Imperial College London, Sidos, Smiths, the Society of Motor Manufacturers and Traders, and University College London

The views and opinions expressed during this discussion do not reflect official or company policy, or the position of Government.