Digital Security Risks to Transport Infrastructure: Automated Vehicles

Henrik Kiertzner – Principal Cybersecurity Consultant, SAS Institute

Threat Actors

- State and quasi-state actors
- Single-issue activists
- “Hobbyists”
- Criminals

Threat Actors – The Evolving Landscape

- Wider access to sophisticated tools and exploits
- Enhanced opportunities for financial gain through crime:
  - Ransom
  - Compromise
  - Theft
- Enhanced opportunities for asymmetric conflict:
  - Disruption
  - Damage
  - Denial

Vulnerability

- End point
- Network
- Control centre
- Design and manufacture

End point vulnerability

- Onboard interface – external or internal attack
- Individual vehicle
  - Control
  - Access
  - Disruption of operation
- Selective/non-selective
- Ransom/kidnapping/theft

Network Vulnerability

- GSM 4G/5G + other radio
- Encryption?
- Jamming?
- Disruption/spoofing
- GPS interference?
- Upstream and downstream interfaces

Control Centre Vulnerability

- Multiple interfaces
- IT/OT
- ‘Conventional’ hacking
- Mass/selective/targeted attacks
- Identity attacks

Design and Manufacture Vulnerability

- Cheap devices
- Embedded firmware
- Patching?
- Multiple version support

Implications

- IoT devices – requirement for scrupulous attention to security in design and manufacture
- Control centres – requirement for high-grade cyber defence and situational awareness + interface hardening at IT/OT interface and at network interfaces
- Networks – requirement for high-grade strong cryptographic protection of network traffic, for resilient communications and safe autonomous operation if network compromised or unavailable
- End points – strongly secured, physically and virtually. Identity-based access?