Session 2: Panel: Cyber Attacks on Safety-Critical AV Functions: Technology & Policy

Session Chair: T. Basil Smith, Rapporteur: Wilfried Steiner

The 2nd IFIP Workshop on Intelligent Vehicle Dependability and Security (IVDS)

Panelists

- Cybersecurity for Connected and Autonomous Vehicles
  - Kristie Pfosi, Director of Product Cybersecurity, Aptiv
- Managing Legal Consequences from Cyber Attacks on Safety-Critical Functions of Intelligent Vehicles
  - William Widen, Professor of Law, Univ of Miami School of Law
- Cross-Collaborating to Secure Autonomous Ground Vehicles and Other Emerging Technologies Against the Threats of Tomorrow
  - Benjamin Gilbert, Cybersecurity Advisor (CSA) in US Department of Homeland Security
- Panel Discussion

Cybersecurity for Connected and Autonomous Vehicles, Kristie Pfosi, Director of Product Cybersecurity, Aptiv

- Aptiv is Tier1 supplier to most major OEMs their components are integrated by the OEM.
- Today, cars have 120-200 ECUs w/ in total >100MLoC. Implies potentially high number of SW bugs.
- Auto has some unique challenges that cannot be addressed by out-of-the-box security solutions.
    - Example: right to repair, 12y average life time, must operate in all global environments.
- Security culture has to be established in the auto industry
    - Training of 10,000 engineers to follow cybersecurity best practices.
    - A lot of industry is not ready for the SW-defined car, e.g., “silent recall” by an OEM via OTA update.
    - The 2015 Jeep hack has caused the first non-safety recall. In retrospect, some question this decision.
    - Since then, many cybersecurity events and reports have not resulted in recalls.
- The auto industry is missing cybersecurity guidance, e.g., in vulnerability and risk management.
- Efforts of chip vulnerability at a Tier1: report of chip vulnerability – ~20 products affected at 12 different customers – impact analysis limited to component level b/c of missing system-level insight – 1 customer may require a mitigation.
- AUTO-ISAC publishes best practices and have monthly calls very suitable to engage with researchers.
- Women’s Security Alliance

Managing Legal Consequences from Cyber Attacks on Safety-Critical Functions of Intelligent Vehicles, William Widen, Univ of Miami School of Law

- Focus on negligence, which is the failure to exercise reasonable care.
- Auto hesitance to regulation because of potential negligence, similar w/ standards.
- A jury will decide if it is a case of negligence.
- Discussion of items that likely affect jury decision:
  - Auto industry creates knowledge that problem exist, what mitigation has been done?
  - Why would the industry not follow their own standard?
  - Standard had to be completed b/c of time pressure, maybe not a good argument.
  - Disproportionate testing in areas of vulnerable communities.
- Some failures stand out, e.g., no blue/red team, insufficient attention on the risk from the supply chain.
- Learning from the financial sector: gatekeepers were insufficient.
  - Mitigation: CEOs have to sign off procedures. Auditing by a third party is recommended.
- Parallels of automotive AV to learnings from the railway industry.

Cross-Collaborating to Secure Autonomous Ground Vehicles and Other Emerging Technologies Against the Threats of Tomorrow, Benjamin Gilbert, Cybersecurity Advisor (CSA) in US Dep. of Homeland Security

- Cybersecurity and Infrastructure Security Agency (CISA), one of the newest agencies in federal government.
- Shields-up Campaign launched as a response to increase in geopolitical threats and increased threats from organized crime (Ransomware-as-a-service). Create awareness and Call for Action.
  - Call to lower reporting thresholds – report to FBI or CISA.
- Two (out of five) operation priorities discussed in detail:
  - (i) Cyber Supply chain and 5G: supply chain attacks have risen; 5G risk from adversary countries.
  - (ii) Industrial Control Systems: Operational Technology (OT) systems are often high-integrity high-availability for the protection of people; traditionally a focus on safety but not security; issue of “insecurity by design”; cascading impact of an incident;
- CISA offers no-cost cybersecurity services.
- Autonomous Vehicle Cyber-Attack Taxonomy (AV|CAT)

Panel Discussion

- Cyber-Attack Taxonomy can be applied to different domains but some attack vectors are specific to ground vehicles.
- Continued discussion of jury behavior:
  - Jury will likely be non-experts following a debate between competing experts.
  - OEMs may follow a bad strategy right now: generating standards but not following them.
- Industry adoption of standards and methods:
  - The OEM declares which level of automation the AV is. Different OEMs have different names for similar features which makes it hard for a consumer to compare.
  - ISO 21434 is getting adopted. It affects many existing process documents and requires new ones. However, it is more a process standard and lacks prescriptive methods.
  - Auto industry implements security methods like encryption, certificates, authentication handshakes, and secure gateways. However, typically no replication nor redundancy is used for cybersecurity mitigation.
  - Auto prefers to adopt solutions from other industries (including learnings from Microsoft) but not everything works out of the box due to industry-specific requirements.
- Question left open: what is the definition of an autonomous vehicle?