Vehicle-to-Infrastructure Cybersecurity: Securing Transportation's Future

P2P3-R07: Vehicle-to-Infrastructure Cybersecurity: Securing Transportation's Future

Christopher Waters, Cyber Solutions Technical Leader, GDIT

Vehicle-to-Infrastructure Cybersecurity: Securing Transportation's Future

How do connected and autonomous vehicles interact securely with transportation infrastructure? This cybersecurity topic, dubbed vehicle-to-infrastructure (V2I) security, was broached during an RSA 2019 Peer2Peer session. Earlier in the conference (https://www.rsaconference.com/blogs/driving-toward-safety-automotive-industry-struggles-with-security-in-rolling-out-connected-vehicles), Ed Adams and Larry Ponemon stated that 84% of those surveyed from the automotive industry are concerned that cybersecurity is not keeping pace with technology. Peer2Peer attendees from academia, government and industry raised key current security challenges and future challenges, with the latter not fully understood today of course. Although one hour only scratched the surface of this emerging security area, commonalities with long-standing security themes are clear.

Vehicles and their passengers will rely on commercial infrastructure such as roadside equipment, intelligent traffic lights and cloud-based data sources. Security of this infrastructure will require strong partnerships between industry, who builds and operates infrastructure, and governments at all levels, who purchase and manage the infrastructure. Standards for data and infrastructure devices are critical to getting V2I security right.

The group debated technical matters relevant across cybersecurity such as how much computing power is needed to process high data volumes and how 5G will affect vehicle communications, perhaps positively because vehicles can receive more road map and road condition updates.

Peer2Peer attendees raised privacy issues. How often will vehicle certificates be rotated to protect privacy? Credential policies, including public key certificates and infrastructure, are an active research area. Vehicle data, which might contain PII, will be stored widely. How long will this data be retained across numerous infrastructure devices? Tokenization was offered as an existing measure to help user data privacy.

Overlapping safeguards are vital in V2I security. Much like air bags and seat belts protect passengers now, vehicle safety systems will need multiple security checks to guard against malicious V2I input. Today, malicious input may take the form of modified road signs or camera feeds. In the future, an attacker who attempts denial of service about road closures may be defeated by a connected vehicle's backup data "channel" to receive and verify alerts above a certain priority threshold. Similarly, the potential to spoof traffic signal indicators communicated to a moving autonomous vehicle may reinforce the need for onboard, independent verification by vehicle cameras.

Attendees asked interesting questions that were left open:

* Who assumes risk for security of V2I communications?

* How will connected and autonomous vehicles with V2I communication features integrate on the road with "dumb" vehicles?

Testing of V2I systems is a feature in projects such as Honda's Safe Swarm. As vehicle manufacturers roll out new vehicle features, testing with a variety of devices and data flows is essential to make V2I security as robust as possible.