Photo Source: USDOT

HOW THE U.S. DEPARTMENT OF TRANSPORTATION IS PROTECTING THE CONNECTED TRANSPORTATION SYSTEM FROM CYBER THREATS

LIMIT 35 SAFETY MOBILITY ENVIRONMENT

The last few decades have witnessed the pervasive spread of computers, the Internet, and wireless technology. As these systems have become integral to our daily lives, so too has the potential for attacks to those systems. Cyber security has risen out of necessity to protect these vital systems and the information contained within them.

Photo Source: USDOT

In particular, transportation is becoming more connected and dependent on advanced computing systems and software. Exciting next-generation communications technology—such as connected vehicles that exchange information in real time with nearby vehicles and infrastructure to make travel safer, cleaner, and more efficient—will soon be deployed on nation's roads and highways. In exploring the potential of connected vehicles and other advanced technologies, the U.S. Department of Transportation (USDOT) understands that cyber security has an even more important role—systems, devices, components, and communications must be protected from malicious attacks, unauthorized access, damage, or anything else that might interfere with safety functions.

USDOT takes cyber security very seriously. The Department is committed to ensuring the security and privacy of our connected transportation system.

USDOT's Cyber Security

The USDOT has several research programs dedicated to ensuring a secure connected transportation environment:

- Vehicle Cyber Security – Focuses on preventing attacks from entry into our vehicle systems and components
- Infrastructure Cyber Security – Focuses on protecting against threats and vulnerabilities to our nation's roadside equipment, devices, and systems
- Dedicated Short-Range Communications (DSRC) Security – Focuses on ensuring trusted communications between vehicles and between infrastructure and vehicles
  - Security Credential Management System (SCMS) Operations
  - SCMS Management
- ITS Architecture and Standards Security – Focuses on the development of architecture and standards required to ensure security in the connected vehicle environment.

The Intelligent Transportation Systems Joint Program Office (ITS JPO) is leading research into cybersecurity technical and policy mitigations, in partnership with modal agencies and other Federal agencies, industry, and academia, to ensure that:

- New technologies have security as an inherent part of their design and operations
- A more unified approach to vehicle, device, and infrastructure security is provided for the connected vehicle environment.

Funding modal partners to conduct critical research, deployment, and operational activities to advance cyber security initiatives.

U.S. Department of Transportation

Vehicle Cyber Security

Today's vehicles offer an amazing array of advanced technologies that enhance safety, improve efficiency, and reduce environmental impacts. These are accomplished through increased use of electronics and software in vehicle design and manufacture. However, the same capabilities also introduce new risks involving unauthorized access to vehicle systems to retrieve driver data or manipulate vehicle functionality.

As vehicle cyber security threats have emerged, the National Highway Traffic Safety Administration (NHTSA) has adopted a research approach focusing on solutions to harden the vehicle's electronic architecture against potential cyber-attacks and ensure vehicle systems take appropriate, safe steps, even when an attack may be successful. A layered approach to vehicle cyber security reduces the probability of success for an attack and mitigates the potential ramifications of a successful intrusion.

To learn more about NHTSA's vehicle cyber security research approach and collaborative initiatives, view the fact sheet *NHTSA and Vehicle Cyber Security* at https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity.

Infrastructure Cyber Security

The Federal Highway Administration (FHWA) is working on multiple fronts to improve the cyber security resilience of surface transportation infrastructures. Outreach and awareness efforts are underway in cooperation with the National Highway Institute, engineering organizations, and transportation agencies to demonstrate how cyber security risks can affect their operation. Tools are being created to help interested agencies improve their infrastructure, processes, and organizational structures to more effectively address risk to their cyber physical systems. FHWA's efforts have focused on customizing risk mitigation materials, originally developed by the National Institute of Standards, for operating engineers in the highway transportation sector. The agency also is working closely with the ITS JPO to explore, assess, and mitigate additional risks that potentially could stem from increased connectivity between vehicles and infrastructure.

ITS Architecture and Standards Security

The USDOT has pursued a "security by design" approach to developing the system architecture for connected vehicles — meaning that the entire connected vehicle system (vehicles, roadside components, and communications media) has been designed with the critical goal of cybersecurity in mind.

The Department's vision is to build uniform, end-to-end security into the system architecture to protect the integrity and privacy of the data traveling throughout the connected vehicle ecosystem. This security approach ensures that vehicles exchanging data as they travel down a highway, vehicles receiving data from infrastructure at traffic signals or work zones, and all other components and participants in the connected vehicle system can rely on the integrity of the connected vehicle data received.

The USDOT has supported and participated in the development of voluntary consensus standards critical to the trust/authentication model of security for connected vehicle environments. Organizations such as the Institute of Electrical and Electronics Engineers and the Society of Automotive Engineers develop voluntary consensus standards in cooperation with industry and deployers. The foundational standards required for the USDOT's connected vehicle security solution have been published and are publicly available. The ITS JPO will continue to support and work with these organizations to evolve these foundational standards and develop additional security standards required to ensure security in the connected vehicle environment.

DSRC Communications Security

The ITS JPO and NHTSA partnered with the automotive industry and industry security experts through the Crash Metrics Avoidance Partnership (CAMP) to design and develop a communications security solution for the connected vehicle system, called the Security Credential Management System (SCMS), that can ensure trusted communications between vehicles and between vehicles and infrastructure. An SCMS Proof-of-Concept (POC) was developed to support the Connected Vehicle Pilots and other federally funded vehicle-to-everything (V2X) related efforts. The SCMS POC used a Public Key Infrastructure-based approach that employed highly innovative methods of encryption and certificate management to facilitate trusted communication. Authorized system participants used digital certificates issued by the SCMS POC to authenticate and validate the safety and mobility messages that form the foundation for connected vehicle technologies. To protect the privacy of vehicle owners, these certificates contained no personal or equipment-identifying information but served as system credentials so that other users in the system could trust the source of each message. Each device or user also had a multitude of certificates that the device constantly altered to preserve privacy.

Great strides were made in establishing and operating the SCMS POC. However, to deploy and oversee the multifaceted SCMS, there must be an ownership and governance model(s) to ensure effective governance and continued operations.

While the research was going on, commercial services have become available.

For more information about this initiative, please contact:
Jonathan Walker, Program Manager, Research and Demonstration
ITS Joint Program Office | (202) 366-2199 | jonathan.b.walker@dot.gov |
www.its.dot.gov