Photo Source: USDOT

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

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


Photo Source: USDOT

In particular, the transportation system is becoming more connected by utilizing 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—will soon become ubiquitous on our nation's roads and highways. Connected vehicles and infrastructure will help to reduce crashes, congestion, and greenhouse gas emissions.

In exploring the potential of connected vehicles and other advanced technologies, the U.S. Department of Transportation (USDOT) understands that cybersecurity is a top priority—systems, devices, components, and communications must be protected from malicious attacks, unauthorized access, damage, or disruptions that might interfere with system performance.

The Department is committed to deploying this technology in a manner that ensures the security and privacy of our connected transportation system.

The USDOT's Approach to Cybersecurity

The USDOT has pursued a "security by design" approach to developing the connected vehicle environment—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 USDOT has several research programs dedicated to ensuring a secure connected transportation environment:

- **Vehicle Cybersecurity** – Focuses on mitigating the safety impacts of potential cyber-attacks into vehicle systems and components
- **Infrastructure Cybersecurity** – Focuses on protecting against threats and vulnerabilities to our nation's roadside equipment, devices, and systems

Each year, the Intelligent Transportation Systems Joint Program Office (ITS JPO) and its modal partners conduct research, development, and education activities to facilitate the adoption of information and communication technology to enable society to move more safely and efficiently.

The 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.

U.S. Department of Transportation

- **Dedicated Short-Range Communications (DSRC) Security** – Focuses on ensuring trusted communications between vehicles and between infrastructure and vehicles
- **ITS Architecture and Standards Security** – Focuses on the development of architecture and standards required to ensure security in the connected vehicle environment.

Vehicle Cybersecurity

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 cybersecurity threats have emerged, the National Highway Traffic Safety Administration (NHTSA) has pursued a layered approach focusing on identifying solutions to harden the vehicle's electronic architecture against potential cyber-attacks and ensuring vehicle systems respond appropriately in the event of an attack. This layered approach to vehicle cybersecurity reduces the probability of success for an attack and mitigates the potential ramifications of a successful intrusion.

To learn more about NHTSA's vehicle cybersecurity research approach and collaborative initiatives, view the fact sheet *NHTSA and Vehicle Cybersecurity* at: http://www.nhtsa.gov/staticfiles/administration/pdf/presentations_speeches/2015/NHTSA-VehicleCybersecurity_07212015.pdf.

Infrastructure Cybersecurity

The Federal Highway Administration (FHWA) is working on multiple fronts to improve the cybersecurity 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 cybersecurity 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 and Technology (NIST), for operating engineers in the highway transportation sector. FHWA is also working closely with the ITS JPO and its modal partners to explore, assess, and mitigate additional risks that potentially could stem from increased connectivity between vehicles and infrastructure.

ITS Architecture and Standards Security

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 environment. 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.

In addition, the USDOT had made it a priority to adopt and promote the use of the NIST Cybersecurity Framework (http://www.nist.gov/cyberframework/) within the transportation sector.

DSRC Security

The ITS JPO and NHTSA have partnered with the automotive industry and industry security experts through the Crash Avoidance Metrics Partnership (CAMP) to design and develop a communications security solution for the connected vehicle environment, called the Security Credential Management System (SCMS), that can ensure trusted communications between vehicles and between vehicles and infrastructure. The proof-of-concept version of the SCMS is under development and is expected to be operational in the fall of 2016 to provide security credential materials to early deployments of connected vehicle technology, such as the Connected Vehicle Pilots and Connected Vehicle Test Beds.

What is the SCMS?

Photo Source: USDOT

The SCMS is a Public Key Infrastructure-based security system that ensures trusted and secure vehicle-to-vehicle and vehicle-to-infrastructure communications. The SCMS employs highly innovative methods of encryption and certificate management techniques to enable vehicles and devices unknown to each other to trust and rely on the connected vehicle data exchanged and received on the system. The SCMS is designed to create this secure cooperative environment without compromising the privacy of system participants.

Manufacturers of devices, vehicles, or other physical components critical to this secure cooperative environment will need to demonstrate compliance with required security controls before receiving the credentials required to participate in any trusted communications.

For more information about this initiative, please contact:
Kevin Gay, Team Lead, ITS Policy and Knowledge Transfer
ITS Joint Program Office | (202) 493-0259 | kevin.gay@dot.gov | www.its.dot.gov

FHWA-JPO-11-021