Inland Empire Regional Mobility Dialogue Series

Results and Summary

LTC
Leonard Transportation Center
CAL STATE SAN BERNARDINO

CALIFORNIA STATE UNIVERSITY
SAN BERNARDINO
Jack H. Brown College
Business and Public Administration

HNTB

SBD
International Airport

Cybersecurity & Surface Transportation: Implications Projection

Feb 19, 2019

Introduction

As technological advancements expand, cybersecurity must be taken into consideration to safeguard the transportation infrastructure. The safe and efficient operation of a traffic management system relies largely on the application of advanced technologies. While new technologies have greatly enhanced how traffic signals work and efficiently operate, these technologies have also increased the exposure to numerous cybersecurity threats.

There is this whole new emerging field of cybersecurity related to emerging mobility solutions. As transportation agencies build an advanced and connected traffic signal infrastructure, they are becoming more aware of the potential threats to our systems. This Dialogue looked at the possible surface transportation threats and solutions on how to safeguard the system.

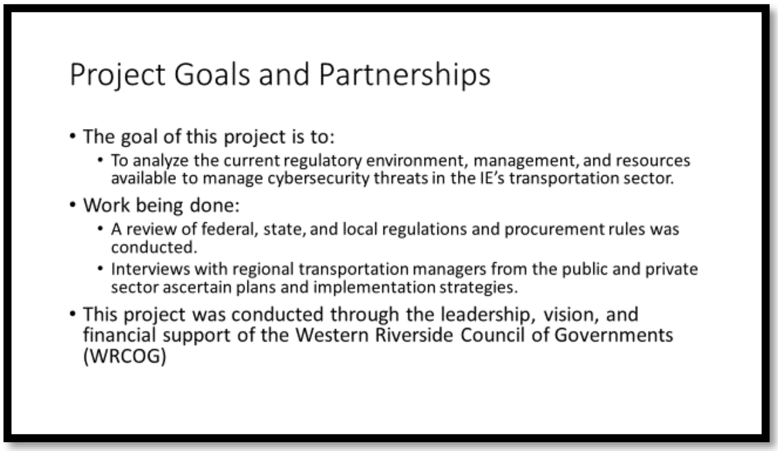
The Dialogue began with a presentation on a study that was conducted by CSUSB's Leonard Transportation Center (LTC). This presentation was followed by a discussion from a private sector expert on cybersecurity. The two thought leaders participating in this discussion were:

- Dr. Montgomery Van Wart, Professor, Project Consultant, California State University San Bernardino
- Kenneth M. Carter, Certified Information Systems Security Professional, Project Management Professional, Cyber Security Engineer, Parsons Corporation

The main takeaways from this discussion include having better vendor management and accountability; and educating the general public with more forums like these, specifically on vulnerabilities of the system, and the necessary precautions to take to help prevent cyberattacks. Moving forward, the Inland Empire must focus on improving the security of the regional infrastructure and addressing cybersecurity issues.

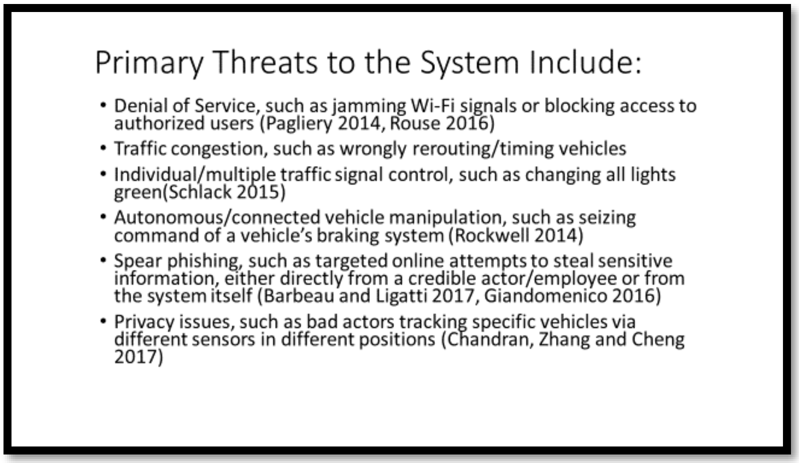
Montgomery Van Wart – Ph.D., Professor, Project Consultant, CSUSB Public Administration

The project undertaken by the LTC focused on the management of surface transportation systems and cybersecurity – an area of study that has remarkably received little attention as it is a low profile public management issue. Information system technologies and applications in the transportation sector provide a number of opportunities in terms of increased efficiency. The major benefits being increased safety and efficiencies, but with that has come enormous challenges in terms of cybersecurity management. Dr. Van Wart and the CSUSB research team interviewed local agencies, met with experts across the country, and conducted a literature review to explore the issue of cybersecurity and transportation.



Project Goals and Partnerships

- The goal of this project is to:
  - To analyze the current regulatory environment, management, and resources available to manage cybersecurity threats in the IE's transportation sector.
- Work being done:
  - A review of federal, state, and local regulations and procurement rules was conducted.
  - Interviews with regional transportation managers from the public and private sector ascertain plans and implementation strategies.
- This project was conducted through the leadership, vision, and financial support of the Western Riverside Council of Governments (WRCOG)

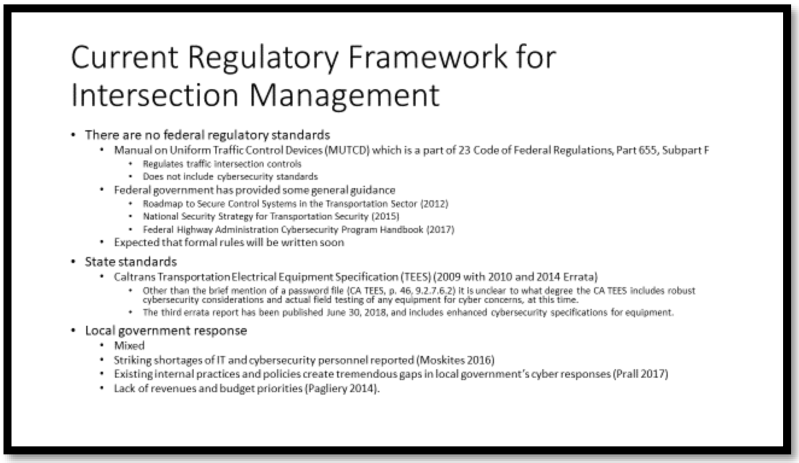


Primary Threats to the System Include:

- Denial of Service, such as jamming Wi-Fi signals or blocking access to authorized users (Pagliery 2014, Rouse 2016)
- Traffic congestion, such as wrongly rerouting/timing vehicles
- Individual/multiple traffic signal control, such as changing all lights green(Schlack 2015)
- Autonomous/connected vehicle manipulation, such as seizing command of a vehicle's braking system (Rockwell 2014)
- Spear phishing, such as targeted online attempts to steal sensitive information, either directly from a credible actor/employee or from the system itself (Barbeau and Ligatti 2017, Giandomenico 2016)
- Privacy issues, such as bad actors tracking specific vehicles via different sensors in different positions (Chandran, Zhang and Cheng 2017)

There are a variety of threats to the system, but most local cities do not have enough staff to ensure security of the transportation systems. "This becomes particularly important at the local government level, all small agencies have challenges trying to get the level of expertise that they want on specialized issues," said Van Wart. Many cities have to rely on industry vendors to ensure that the equipment provided is secure. "If we are not very careful, what we find is with the product or services we order, we don't always get what we are promised," shared Dr. Van Wart.

Some of the specific challenges that the devices face in intersection management is they frequently have low levels of cybersecurity built into them, and some of the legacy devices are commonly devoid of security. Over time many of these systems are being replaced with higher levels of security. Cyber threats to transportation management systems are not only introduced by way of individual devices, but through the amalgamations of various devices and systems that provide nexus-point vulnerabilities. "The industry has been slow to respond and be proactive in providing security controls to anticipate the next phase of black hat hacking," said Van Wart. Black hat hacking is a term used to describe an individual who attempts to locate computer security vulnerabilities and exploit them.



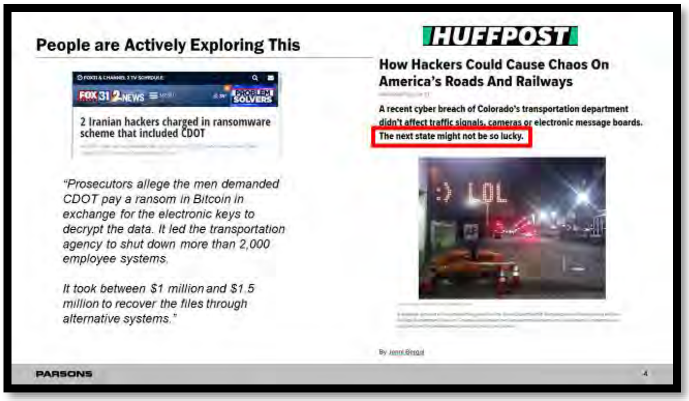
Current Regulatory Framework for Intersection Management

- There are no federal regulatory standards
  - Manual on Uniform Traffic Control Devices (MUTCD) which is a part of 23 Code of Federal Regulations, Part 655, Subpart F
    - Regulates traffic intersection controls
    - Does not include cybersecurity standards
  - Federal government has provided some general guidance
    - Roadmap to Secure Control Systems in the Transportation Sector (2012)
    - National Security Strategy for Transportation Security (2015)
    - Federal Highway Administration Cybersecurity Program Handbook (2017)
  - Expected that formal rules will be written soon
- State standards
  - Caltrans Transportation Electrical Equipment Specification (TEES) (2009 with 2010 and 2014 Errata)
    - Other than the brief mention of a password file (CA TEES, p. 46, 9.2.7.6.2) it is unclear to what degree the CA TEES includes robust cybersecurity considerations and actual field testing of any equipment for cyber concerns, at this time.
    - The third errata report has been published June 30, 2018, and includes enhanced cybersecurity specifications for equipment.
- Local government response
  - Mixed
  - Striking shortages of IT and cybersecurity personnel reported (Moskites 2016)
  - Existing internal practices and policies create tremendous gaps in local government's cyber responses (Prall 2017)
  - Lack of revenues and budget priorities (Pagliery 2014).

Current Federal guidance on cybersecurity is generic. The testing of equipment often comes from state agencies. It is uncertain how in-depth their testing is, specifically related to program error detection that can lead to vulnerabilities. Qualified product lists, generally adopted by local governments from the state level, do not provide any information or guidance other than acknowledgement that they have been found to be acceptable on a number of engineering aspects, one of which is cybersecurity. "It is just saying there are only recommendations and they only have so many resources. Caltrans only has so many resources to devote to this particular area and cyber is only one aspect of all the device testing that they do," said Van Wart.

<u>Kenneth Carter- CISSP-ISSEP, ISSMP, PMP, GCIA, Cyber Security Systems Engineer, Lead, Parsons Plus</u>

Kenneth Carter, Cyber Security Engineer with Parsons Corporation, discussed threats and attacks in transportation systems, the target environment, and what the compliance landscape looks like. Parsons is an architecture and engineering firm that is often contracted to work on transportation systems. Due to a lack of security measures, people can actively exploit transportation systems for financial gain or other malicious reasons. “The state of Colorado Department of Transportation (DOT) had a pretty big attack not long ago. The way ransomware typically works is they try and trick somebody into downloading something or opening an email attachment. Once opened it gets into your environment and tries to spread,” Said Carter.



People are Actively Exploring This

FOX31 2NEWS PROBLEM SOLVERS

2 Iranian hackers charged in ransomware scheme that included CDOT

“Prosecutors allege the men demanded CDOT pay a ransom in Bitcoin in exchange for the electronic keys to decrypt the data. It led the transportation agency to shut down more than 2,000 employee systems.

It took between $1 million and $1.5 million to recover the files through alternative systems.”

HUFFPOST

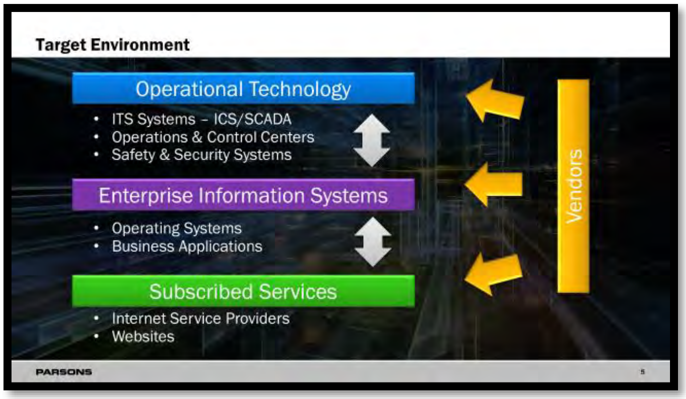
How Hackers Could Cause Chaos On America’s Roads And Railways

A recent cyber breach of Colorado’s transportation department didn’t affect traffic signals, cameras or electronic message boards. The next state might not be so lucky.

By Jenni Bergal

PARSONS 4

When Colorado’s DOT got hit, thousands of machines were taken offline. Once the virus was inside the system, it affected nearly half its computing environment, around 400 servers, all databases and applications, and around 1,300 workstations. “Colorado a couple years ago, went through an exercise to save money and consolidate the backend IT systems. They use to have a server room that was about the size of these two conference rooms here, just loaded with IT equipment. By the time they consolidated everything it was down to about two racks,” said Carter. All state emails were on those machines, so if these machines are hacked the repercussions can be devastating. It cost the state of Colorado a little over a million dollars to remediate all the damage done.



Target Environment

Operational Technology
- ITS Systems – ICS/SCADA
- Operations & Control Centers
- Safety & Security Systems

Enterprise Information Systems
- Operating Systems
- Business Applications

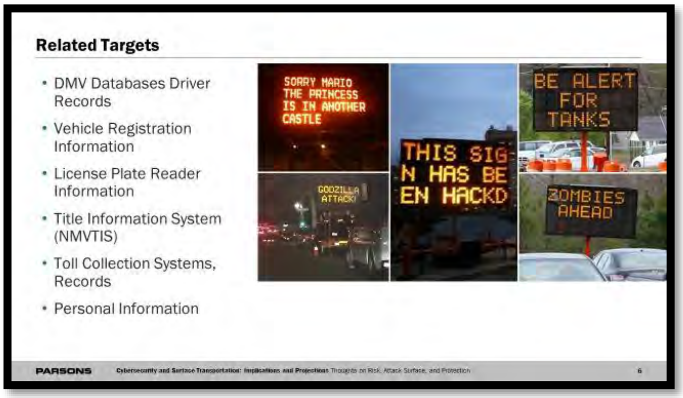
Subscribed Services
- Internet Service Providers
- Websites

PARSONS 5

When looking at the target environments, there is:

- Operational Technology
- Enterprise Information Systems
- Subscribed Services

The transportation equipment that is the easiest to hack is the road sign. “I've actually done this myself in a controlled environment, and with permission,” said Carter. One easy way to prevent attacks is to simply lock the control panel on the sign.



Related Targets

- DMV Databases Driver Records
- Vehicle Registration Information
- License Plate Reader Information
- Title Information System (NMVTIS)
- Toll Collection Systems, Records
- Personal Information

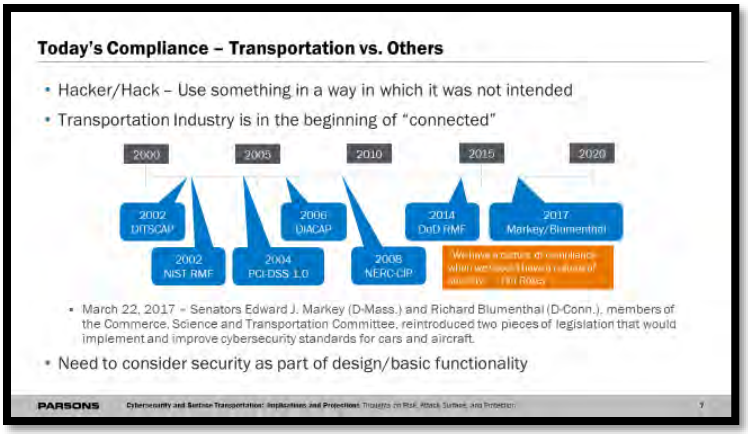
SORRY MARIO THE PRINCESS IS IN ANOTHER CASTLE
GODZILLA ATTACK
THIS SIG N HAS BE EN HACKD
BE ALERT FOR TANKS
ZOMBIES AHEAD

PARSONS Cybersecurity and Surface Transportation: Implications and Projections Thoughts on Risk, Attack Surface, and Protection 6

Today, there is connectivity between our systems that didn’t exist up until about five years ago, and the operational technology systems that were once considered safe from hacking, are no longer safe. “One of the big things we find when we go out and do assessments for clients, is there is a lot of undocumented connections. Companies will set up some kind of temporary connection, which if you've done any work for the federal government, nothing's more permanent than a temporary connection,” said Carter. The problem with undocumented connections, is they are less secure and there is a higher risk of people gaining unauthorized access because they are no longer a closed network. Something that was intended to be a temporary connection, has now become a permanent connection. Due to this remote access, the systems become more vulnerable to cyberattacks.

With these types of systems, hackers are often looking to outdo the last hacking attempt. They want to show off, or pull off the grander attack. They get bored with hacking traffic signs and are looking at bigger things like, highways, public information systems, railways, or airports. Some of these are harmless attempts, but when we look at the larger scale, there are always those out there who have malicious intentions. “What happens if an attacker gets into the road signs, let's say along all the highways here in LA, and it says chemical attack, seek shelter,” said Carter. This could cause massive panic.

Another target susceptible to attacks is payment card systems. There is a substantial amount of risk with online payment methods, for example, when a customer makes an online purchase their bill gets sent to a third party provider to process the charge. This is where there is a lot of risk and exposure to personal information. There are couple of rail agencies here in the United States that use remote vendors (third party consultants), and these vendors will conduct updates to their systems that are not appropriately coordinated with the rail agencies. The rail agencies are assuming that the vendors are going to do the job right, but that is not always the case. The vendors do not always use the correct procedures when performing these updates, ultimately leaving the rail agencies’ systems compromised.



Today's Compliance – Transportation vs. Others

- Hacker/Hack – Use something in a way in which it was not intended
- Transportation Industry is in the beginning of “connected”

- March 22, 2017 – Senators Edward J. Markey (D-Mass.) and Richard Blumenthal (D-Conn.), members of the Commerce, Science and Transportation Committee, reintroduced two pieces of legislation that would implement and improve cybersecurity standards for cars and aircraft.
- Need to consider security as part of design/basic functionality

PARSONS Cybersecurity and Surface Transportation: Implications and Projections Thoughts on Risk, Attack Surface, and Protection 7

In addition to payment card systems, another big concern is autonomous vehicles. As these autonomous vehicle systems start to talk to each other and share information with one another, this leaves an open window for hackers to access personal information such as, names, addresses, and date of birth.

In 2000, the compliance landscape for the U.S. Department of Defense started enforcing rules and regulations on how to secure government IT systems and military systems. It is important to start thinking about safeguarding our transportation systems. The American Public Transportation Association (APTA) is starting to put together cyber specific standards for transportation, rail, aviation, and intelligent transportation systems. Overall, cybersecurity needs to be incorporated into all future operational designs to further protect and safeguard our IT systems.

Moving the Dialogue Forward: Ideas from the Participants

After the presentations, dialogue attendees discussed the ideas presented and worked together in groups to discuss solutions to move it forward. The top three ideas from each table have been categorized and summarized below.

Better accountability and practices for vendors. A number of participants discussed how there needs to be better management and vendor practices for cybersecurity risks.

- Hold vendors responsible for their security protocol.
- A better system needs to be put into place in order to monitor industry vendors.
- Assess what systems are already out there, including specific vendors.
- It would be a good idea to have a vendor fair or expo, so that we can meet the vendors to assess their reliability.
- Sorting through vendor procurement to make sure they are following specific security measures.
- Better vendor vetting.

Educating the public on cybersecurity risks and conduct analysis of systems out there. Some of the participants mentioned how the general public needs to be better informed on the cybersecurity risks out there and in order to educate people, we need to assess what systems are currently utilized.

- We need to have cyber education: How can higher education push transportation and cybersecurity?
- How can we make the general public more aware of how vulnerable our systems are and how to take the necessary precautions?
- We need to become more aware of our server systems.
- It is important to educate and stress the importance for cybersecurity analysis to agencies.
- Continue to hold more forums like these to help educate community members and stakeholders.
- Have IT training/cybersecurity training for employees in our agencies and trainings with other organizations.
- Assess what others are doing locally, regionally, statewide and nationally.
- Move forward with technical demonstrations to educate people on how easy it is for our system to be hacked and how to take precaution.

Making sure government leaders are aware of potential threats and implement security measures accordingly. A few of the participants were interested in knowing what role our local government leaders play in safeguarding our systems.

- We should be sure to inform local government leaders on the potential threats to our systems and be better equipped to prevent hacking.
- Make sure local leaders are aware of sensitive server information.
- Enforce higher security and testing of our systems.

The Leonard Transportation Center (LTC) at California State University San Bernardino (CSUSB), presented a bi-monthly dialogue series on topics relevant to the future of transportation in the Inland Empire. The series, which was open to the public, was sponsored by HNTB Corporation and was held every other month starting in February 2018.

Dialogue topics ranged from understanding the current mobility dilemma and its causes to potential solutions like congestion pricing, transit; emerging technologies such as autonomous and connected vehicles and new ways of funding transportation infrastructure. Attendees had the opportunity to hear from transportation experts and engage in vigorous discussion about the transportation challenges facing the Inland Empire.

About Leonard Transportation Center

The Leonard Transportation Center (LTC) at California State University, San Bernardino opened in 2006 with a focus on regional transportation needs. The vision of Bill and Barbara Leonard was to create a center that focuses on the unique transportation opportunities and challenges the Inland Empire faces. Today, the LTC is working to expand its research and student engagement programs. Focal points include transportation management and governance issues, development of new technologies, and transnational studies. Their vision is to work collaboratively to seek solutions to assist residents, businesses, government and nonprofit agencies, and international partners to work together on improving sustainability and quality of life in the Inland Empire. For more information, visit www.csusb.edu/ltc.

About HNTB

HNTB Corporation is an employee-owned infrastructure solutions firm serving public and private owners and contractors. HNTB's work in California dates back to its founding in 1914. Today, HNTB continues to grow in size and service offerings to clients in California from seven office locations, currently employing more than 350 full-time professionals. With more than a century of service, HNTB understands the life cycle of infrastructure and addresses clients' most complex technical, financial and operational challenges. Professionals nationwide deliver a full range of infrastructure-related services, including award-winning planning, design, program management and construction management. For more information, visit www.hntb.com

About San Bernardino International Airport

Conveniently located in the heart of the Inland Empire, close to major freeways and just 60 miles from Los Angeles, San Bernardino (SBD) International Airport is strategically positioned to meet growing aviation activity, including cargo, business aviation, general aviation, and commercial airlines by providing competitive rates for aviation companies and local businesses looking to stretch their wings and expand their horizons. With extensive stretches of pristine runway and acres of prime land available for aviation development, SBD International Airport is ready to help our community and region reach new destinations.