Integration of Technology & Security for the Future of Transportation

May 16, 2017

Charles Chen
Devin Liddell
Sam Chughtai

CASCADIA PACIFIC

Presenters

Devin Liddell	- Teague
Scott MacInnes	- Teague
Warren Schramm	- Teague
Sam Chughtai	- Cascadia Pacific
Charles Chen	- 

CASCADIA PACIFIC

Evolution of roads

Formally just a clearing path, transition to pebble and stone roads

Industrial evolution - paved roads for automobiles, railroads for trains

New way of thinking: it’s not just how well we engineered roads, it’s what is riding on it, what is under it (sensors, fiber optics, electricity) and what is around it (sensors, signals, safety barriers)

CASCADIA
PACIFIC

New way of thinking about roads

How will we use the new high technology roads? How does it improve safety, efficiency, and the environments?

What are we putting on the roads? Let's think about it outside the box. The unimaginable is already coming...

How does new high tech roads tie together with Smart City and Smart Grids, IoT (Internet of Things)?

CASCADIA
PACIFIC

New way of thinking about roads

Let’s think of the revolution of transportation infrastructure in a way that we can relate to:

Historical:

Current:

Future:

CASCADIA PACIFIC

TEAGUE questions

What should be the State’s role within the management and utilization of autonomous vehicle (AV) fleets? That is, should the State be an owner? A regulator? A licensor? A partner?

What are the implications for data ownership within each of the State’s potential roles in managing AV fleets?

CASCADIA PACIFIC

TEAGUE questions, continued

How should the State anticipate interrelationships between public and private AV applications (when an AV acts as a “public” form of transportation vs. when an AV is a “private” service), as well as the interrelationships between public and private transportation modalities (e.g., how AVs relate to and interact with buses, bikes, etc.)?

What policy considerations should be made in terms of how cities are “zoned” for AV fleets?

CASCADIA PACIFIC

TEAGUE questions, continued

What policy considerations should be made in terms of governing standards of user experience? And how do these considerations reflect our position on technologies, socio-economic issues, rights of ways, etc.?

CASCADIA
PACIFIC

Cascadia Pacific:
New Technologies, New Challenges

Cyber security for asphalt and concrete? Don’t be ridiculous… wait...

 How do we protect new infrastructure technologies from a cyber security perspective? No such thing as an Anti-Virus for sensors

Who do you trust? Do you believe in a used car salesperson?

Smart City Transport System Are Vulnerable to Hackers!

Recent News of System Hacks

- BC News, August 5th, 2016,
  New Jersey photojournalist Lori Nichols to turn her car around on a highway near Atlantic City close to midnight to snap a photo.
  http://www.bbc.com/news/business-36854293

- On November 25th, 2016 the San Francisco Municipal Transportation Agency (MUNI) was hacked, shutting down ticketing systems and compromising more than 2,100 of the agency's computers as cybercriminals demanded payment of $70,000 in ransom, forcing the agency to operate free service for two days.

- In 2014, a University of Michigan team accessed a traffic light network using readily available hardware. Once inside the system, the team quickly gained the ability to change traffic signals, alter logic commands and disable signal devices.

CASCADIA
PACIFIC

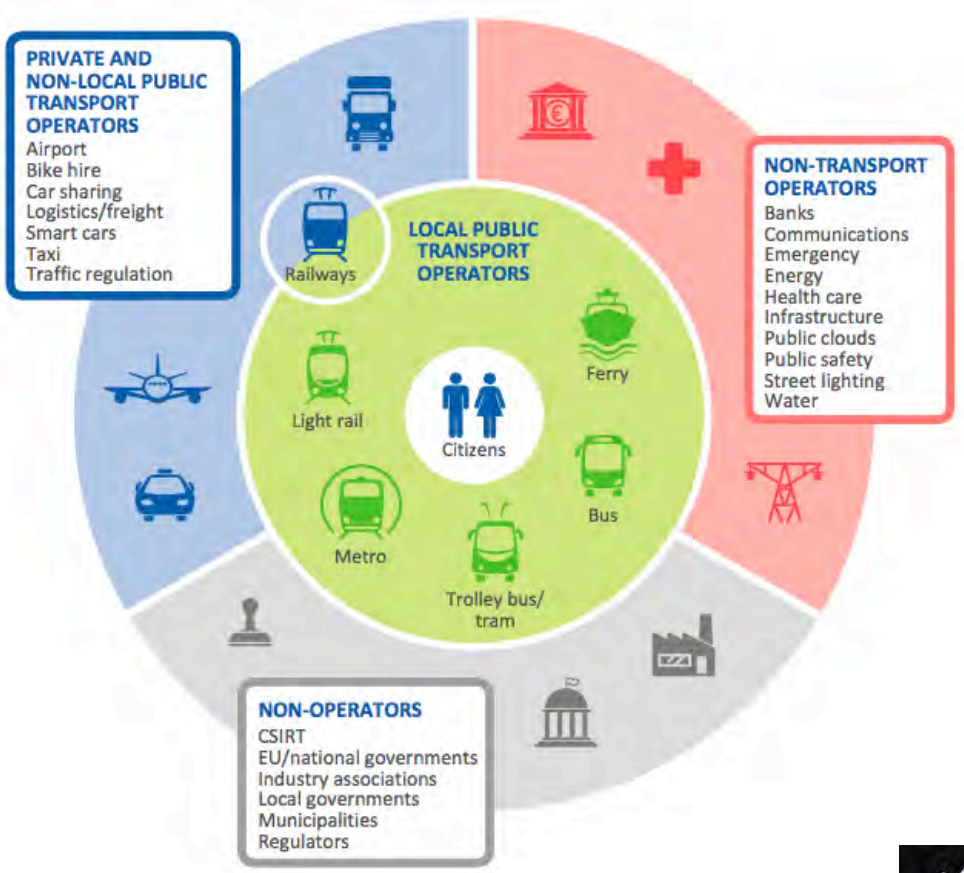
A Page from EU Smart Transportation Policy

*Every device or sensor that connects to the network **broadens the attack surface**, creating a potential entry point for cybercriminals to hack to or hack through. Without advanced cybersecurity, unauthorized access to critical systems, information theft and malicious cyberactivity will thrive in the future's ultra-connected, highly automated and data-driven environment.*

- **Operators:** they cover a wide range of actors; both those directly involved in operating different public transport modes (metro, bus, tram/trolley-bus, light rail, ferry) and an interconnected network of operators within the Smart City (energy, infrastructure, public & private clouds, communications, banks and payment systems, etc.).
- **Manufacturers:** Covering the full spectrum of manufacturers including physical transport infrastructure, providers, vehicle manufacturers, developers of ICT networks, hardware and software engineers, etc.
- **Service Providers:** Including risk managers, cloud providers, ICT network providers, security providers, etc.
- **Policy Makers:** Different levels of government (local, national, EU), regulators and law enforcement agencies involved in IPT.

CASCADIA PACIFIC

Smart Transportation Participants & Data Life Cycle



CASCADIA PACIFIC

Cyber Security for Smart Transportation

Five Cyber –technologies that will be part of the future smart city transportation systems are:

1- Autonomous Vehicles

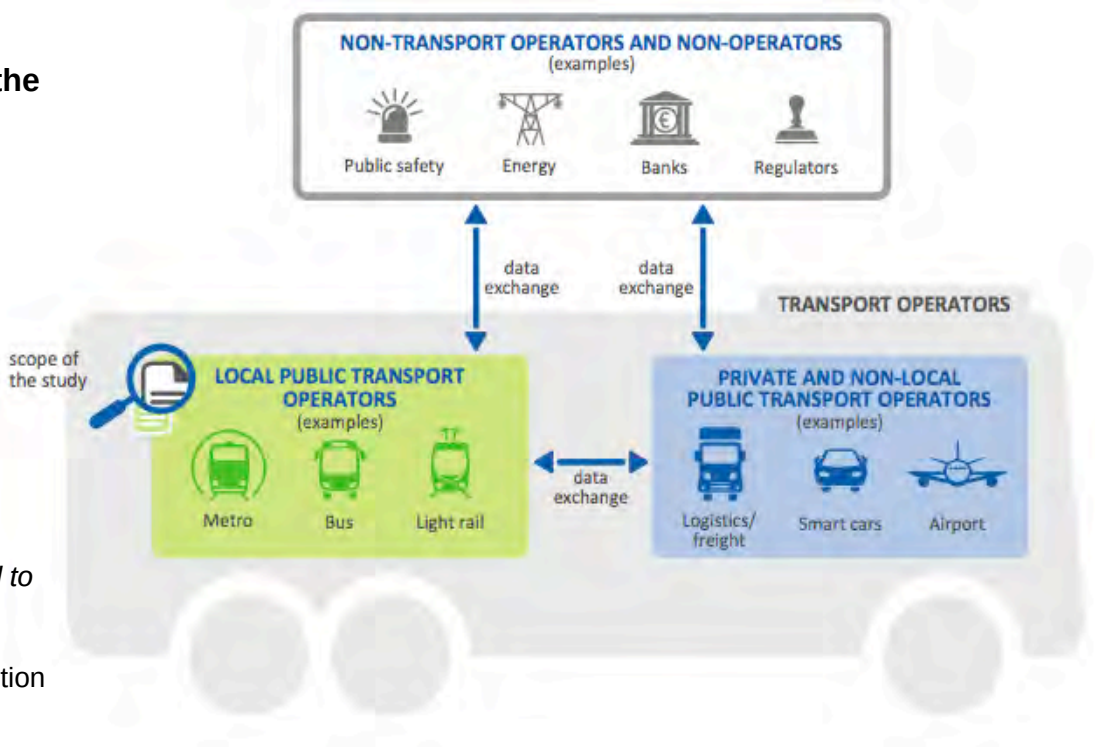
2- Positive Train Control Systems (PTC)

3- Intelligent transportations systems, (ITS)

4- Vehicle to vehicle (v2v)

5- Vehicle to Infrastructure technologies (v2v)

(PTC is a set of highly advanced technologies designed to make freight rail automatically stopping a train before certain types of accidents occur. Its monitoring and controlling train movements and is a type of train protection systems.)



Smart Transportation Inherent Security Risk

- Sheer scale and complexity of transportation networks in major cities, including the difficulty of securing mobile device connectivity to transportation networks and distinguishing legitimate mobile device queries from anomalies.
- Large number of system access points stemming from the presence of networked technology across large systems, raising the cost and difficulty of properly securing each system device. This number includes hardwired access points—many of which may be located in remote areas—and wireless access points.
- Burden of ensuring smooth interface, communication, and security among multiple interdependent systems, including sensors, computers, fare collection systems, financial systems, emergency systems, ventilation systems, automated devices, power relays, etc.
- Demand for nonstop access to real-time data that Smart City transportation systems require, and the related costs associated with maintenance and service downtime.
- Logistical and security hurdles of physically accommodating enormous volumes of passengers and freight, along with the reality that security breaches could result in public safety risks.

CASCADIA
PACIFIC

Industrial Control Systems

Cascadia Pacific - We are the ICS control penetration tester and auditor (smart transportation).

We try to break things to make sure it can’t be broken

We provide an independent internal cyber security assessment and validation of what vendors and suppliers promise you

In Emoji language: We are your 👀 to ✓ and gives a 👍, 👎 or 👌

CASCADIA PACIFIC

Industrial Control Systems - Continued

Where can we find ICS cyber security assessment professionals? Actually, it does not really exist...

Bring the discipline of financial audits into the IT Security domain

Perspective: CIO and CISO point of view? Third party independent auditors to provide confirmation or alternatives

Example: In accounting (1) internal CFO (2) internal audit (3) external audit

CASCADIA
PACIFIC

ICS Assessment and Audit Roadmap

Our approach

The ICS Healthcheck applies an ICS risk analysis and threat modeling methodology followed by technical data analysis.

CASCADIA
PACIFIC

Risk Analysis and Threat Modeling

Document current network

Consultants inventory and review your existing architecture documentation, communications protocols and security policies, and procedures to understand of your ICS security environment.

Develop threat model

Experts work with your IT, operations and engineering staff to identify the high-likelihood and high-risk attack vectors, target and perform pen testing.

Prioritize controls

Using the threat model, our professionals help your team select and prioritize security controls risk mitigation

CASCADIA
PACIFIC

ICS Assessment and Audit Roadmap

Technical data analysis

1. **Review network segmentation**
2. Our consultants deploy a Network Forensics Platform device on your network and then analyze network packet capture files to determine the types of security risks you face
3. **Review security device configuration**

Deliverables

Threat model diagram

ICS Health Check report and Network / Devices Penetration Testing

Strategic and technical recommendations

CASCADIA PACIFIC

Questions?

We know you have lots of questions

If you don’t have any questions… then we failed, or they ran out of coffee

How to reach us? To ask more questions...

CASCADIA
PACIFIC

Contact Information

Sam Chughtai	- Cascadia Pacific	samc@cascadiapacific.com
Devin Liddell	- Teague	dliddell@teague.com
Scott MacInnes	- Teague	smacinnes@teague.com
Warren Schramm	- Teague	wschramm@teague.com
Charles Chen	- 🇺🇸	chencc3@america.gov

A Cyber Security Consulting Company, highly specialized in ICS control penetration testing, security audits, security architecture design and regulatory compliance audit.