UTC Spotlight

University Transportation Centers Program

This month: September 2018

Mineta Transportation Institute at San Jose State University, as part of the Mineta Consortium for Transportation Mobility

U.S. Department of Transportation

Office of the Assistant Secretary for Research and Technology

No. 126

Managing Cyber Risks & Business Exposure in the Surface Transportation Ecosystem

Transportation technology has progressed by leaps and bounds in the past few years and more and more of the physical elements of surface transportation systems are now controlled via Internet connections. But with legitimate remote access comes malicious attempts to gain illegitimate control through cybersecurity breaches. If these attempts are successful, then whole transportation systems have the potential to be compromised.

Odometer. com

Hacked traffic road sign.

A recent project by the Mineta Transportation Institute (MTI) at San Jose State University takes an in-depth look at this phenomenon. Specifically, it looks to address not only how to protect against cybersecurity attacks on surface transportation targets, but also what to do when they are successful. The main goal of this project is to create a holistic transportation cybersecurity management model that assigns responsibilities to each transportation department before, during, and after cybersecurity events.

Breaches Everywhere

The need for better cybersecurity in surface transportation is clear, as evidenced by recent attacks. For example, in 2016, ride-hailing giant Uber paid hackers $100,000 to delete 57 million stolen driver and rider accounts. In the same year, hackers attacked the San Francisco Municipal Transportation Agency (SFMTA), breaking into more than 2,000 servers and holding the data at a $70,000 ransom.

It's not just companies' and organizations' data that are at risk; physical components are at risk also. A 2011 infection of an unspecified northwestern rail company disrupted railway signals for two days. In 2014, researchers hacked into a Michigan network of traffic lights, gaining control of almost 100 intersections. They reported a "systemic lack of security consciousness." These physical components are the last frontier of transportation safety – if they can be hacked, what cannot?

Kimberly-Veklerov

San Francisco Municipal Transportation Agency (SFMTA) ticket kiosk.

Prevention and Mitigation

The first stage in protecting transportation systems from cyberattacks is preventing them in the first place – the 'before' phase. The goal is to stop an attack from becoming a compromise. One of the key competencies at this stage is understanding the specific risks that an organization faces, and subsequently understanding the potential motives of a hacker.

Once the appropriate security measures have been put in place, however, little more can be done to guard against hackers. Additional security protection in the 'before' stage follows a pattern of diminishing returns; each additional resource devoted to protection results in decreasing marginal security gained. The possibility of a successful attack will always remain.

When an attack is successful and hackers are able to enter the system, the 'during' stage starts. The main goal of this stage

MTI

Cyber attack response model.

is to prevent the attack from escalating into a breach, where critical systems are affected or data is stolen. Rather than try and immediately take out the hacker, it is usually best to track them and understand their intent.

When a breach occurs, the 'after' phase comes into play. The key competencies at this stage are handling media and legal fallout, addressing legal claims, and rebuilding infrastructure to prevent like attacks in the future. The effects of particularly damaging breaches can last years.

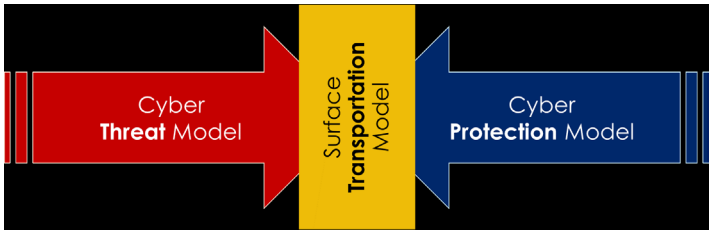
Surface Transportation Cyber-Protection Model and Reference Architecture

To help surface transportation companies and organizations better deal with cybersecurity vulnerabilities, MTI developed a Surface Transportation Cyber-Protection Model. The model's goal is to help create safer, more reliable, and more resilient transportation systems. To do so, it provides methods to model transportation-specific threats, identify areas with the greatest vulnerabilities, estimate risks and financial exposure, and foster an open discussion of existing problems across industry stakeholders.

The model is composed of three key elements: 1) the **cyber threat component** provides the ability to understand potential threats; 2) the **cyber protection component** allows organizations to model courses of action and countermeasures to threats; and 3) the **surface transportation model** identifies the common layers of attack in surface transportation systems.

Each element of the model has an underlying reference architecture, that is, a framework through which the attack is modeled and understood. The cyber threat reference architecture illustrates the steps of a successful cyberattack. Its cyber protection counterpart illustrates how to defend against each one of these steps. The surface transportation reference architecture points to specific infrastructural weaknesses within each layer of a surface transportation system.

In many cases, it is clear that surface transportation systems are vulnerable to malicious attacks and lack cybersecurity protection. By creating a model to better understand and address this issue, MTI will increase the safety and security of all surface transportation systems as their physical infrastructure becomes more and more interconnected. Additionally, it hopes to provide a clear and concise way for individuals at all levels of surface transportation companies and organizations to understand and address existing risks.



MTI

Surface Transportation Cyber-Protection Model

About This Project

Jacques Francoeur, a San Jose State University Faculty Cyber Executive-in-Residence and a Senior Research Scientist for the Mineta Transportation Institute, and Jeremy Steele, a Mineta Transportation Institute intern studying Geography with an emphasis on urban systems and Software Engineering, authored this newsletter. Currently in final publication phase, this research is ongoing. Inquiries may be directed to karen.philbrick@sjsu.edu. More information on this and other projects can be found at: http://transweb.sjsu.edu/mctm/research/utc.

This newsletter highlights some recent accomplishments and products from one University Transportation Center. The views presented are those of the authors and not necessarily the views of the Office of the Assistant Secretary for Research and Technology or the U.S. Department of Transportation.

Printed on paper containing recycled post consumer waste paper.