Guarding against 'Carmageddon' cyberattacks

June 11 2014

The potential value of turning the nation's freeways into "smart transportation systems" is enormous. Equipping the nation's concrete arteries with a nervous system of computers and sensors that directly control on-ramp signals to keep traffic moving smoothly can substantially reduce travel times, fuel consumption and air pollution, not to mention improve road safety. In California alone the economic penalty of traffic congestion has been estimated at $400 million in extra costs and $3.5 million in lost wages every day.

The tightly integrated computing and networking systems required to achieve these benefits are currently under development. But they have a worrisome downside: They are vulnerable to cyber attacks by criminals, terrorists or hostile nations. There was a Hollywood dramatization of this risk in the 2003 movie "The Italian Job" when a hacker takes control of the Los Angeles traffic control system to aid his confederates in stealing a load of gold bullion from an armored car and then escaping.

Developing the means to identify such attacks should they occur and creating software that can guard against them is the goal of the Smart Roads Cyber-Physical Systems project that is being featured at the SmartAmerica Challenge Expo being held on June 11 in the Washington DC Convention Center.

The project is a collaboration between a team of cyber-physical security experts at Vanderbilt University's Institute of Software Integrated Systems (ISIS) and researchers at University of California, Berkeley

College of Engineering and the Partners for Advanced Transportation Technology's Connected Corridors project.

The Connected Corridors team is investigating tools and technologies to coordinate components of major traffic corridors and operate them as a cohesive and integrated system. The first Connected Corridors pilot will be implemented on a multi-modal, heavily congested corridor in Southern California and will include freeway ramp meters and arterial signal systems working in concert with each other.

Under a previous award (FA8750-11-2-0078 from the Air Force Research Laboratory), the ISIS team used advanced computational methods to study how different types of cyber attacks, such as denial of service and spoofing, affect computer networks in general, and they are modifying the methods they developed so they work with the Berkeley traffic control system.

"The immediate object of our project is to identify the characteristics of such attacks so that system operators can recognize them when they happen and take the effective steps required to counteract them," said Gabor Karsai, leader of the ISIS team. "The longer term goal is to develop algorithms that can automatically detect these intrusions and nip them in the bud."

In order to dramatize the problem and potential solutions, the researchers have developed a video scenario titled "Smart Transportation Systems: Mitigating Carmageddon" that depicts how such an attack could take place, the effect it would have on the freeway, as well as the tools that the traffic system operators could use to identify the attack, mitigate its impact and return traffic flow to normal levels.

The scenario begins when a former transportation department employee comes up with a system that turns freeway-metering lights green for the

vehicles equipped with his technology. He sells the system to a local shipping company as a way to cut down on delivery times. He is then approached by a hacker who pays him to add a second device to his system, one that interferes with the communication link between the metering lights and the traffic control center. When enough trucks with this equipment are on the freeway, it gives the hacker virtual control over the traffic system. One weekday morning the hacker uses this capability to bring traffic to a standstill, but the manager of the traffic control center checks on the performance of the metering lights with the traffic cameras, realizes they are misbehaving and launches a set of cyber-security tools that identify the locations where falsified data is being inserted into the system. This allows the controllers to manually control the metering lights, returning traffic to normal.

"Our Smart Roads demo aligns with the goals of the SmartAmerica Challenge," said Alex Bayen, leader of the UC Berkeley team. "Smart transportation systems can decrease congestion, which keeps the economy moving, and make roads safer. Our work focuses on characterizing the impact of attacks on traffic patterns and the potential remediation that would make the system more resilient."

Provided by Vanderbilt University