Security in transportation systems

S. N. Diggavi M. Srivastava P. Tabuada

Networked transportation systems

Over the past few decades, automation has revolutionized transportation, ranging from individual vehicles to traffic networks. Today's cars have sophisticated sensing, actuation and control systems that take several automated decisions on actions such as braking, stability control etc. Similarly, traffic systems use sensors to control traffic signaling. All these advances are leading towards autonomous transportation systems that have had several successful demonstrations [4, 1, 2]. Communication plays a fundamental role in such *networked transportation systems* by coordinating the sensing, actuation, control and computation. However, such advances in networked transportation systems also expose them to security vulnerabilities, both at the cyber as well as at the physical level. These lead to new forms of sophisticated attacks which use the vulnerabilities of both the physical sensing/actuation systems as well as the computing, control and communication systems. This has been demonstrated with dangerous consequences on several models of cars [3, 5]. Vulnerabilities in traffic signaling systems have also been dramatically demonstrated [6]. Within the end of this decade, (partially or fully) autonomous cars will be commercially available, making the issues of security of such systems a critical societal need. In order to defend against attacks which use both the cyber (computing/communication) as well as physical (sensing/actuation) vulnerabilities, one needs a holistic approach using *cyber-physical* security.

Approach to secure transportation systems

Traditionally, cyber-security deals with securing information bits against adversaries. In transportation systems, cyber-security defenses can simply be bypassed by mounting attacks on sensing and actuation mechanisms, since these act on the conversion of physical quantities into bits. Therefore, even the most powerful cyber-encryption scheme would fail when the attacker alters the physical measurement and therefore the input to the encryption scheme. Therefore, security in transportation systems is more than just cyber-security as the objective is to secure the combined operation of the cyber and the physical components. This also gives an opportunity to create new security mechanisms: even when it is not possible to guarantee security of the cyber component in isolation, we may still be able to ensure trustworthy operation of a transportation system by exploiting the interactions between the cyber and the physical components. For example, by utilizing the dynamics of a physical system and the interconnected (correlation of) sensors one can defend against sensing attacks [7]. Therefore, even when individual sensing components can be attacked, like ABS velocity sensors [8], one can secure the system using a holistic approach. Therefore, even when it is not possible to guarantee security of the cyber component in isolation, we may still be able to ensure trustworthy operation of a transportation system by exploiting the interactions between the cyber and the physical components [9, 10].

Networked transportation systems also have a characteristic that sets them apart from several other cyber-physical systems: humans are in the loop. Despite the increase in automation, cars are still driven by humans. Even if we consider the adoption of fully autonomous cars we need to be ready for a future when fully autonomous and human driven cars co-exist. This brings another set of challenges since the modeling of human behavior is difficult for several reasons including culture, physical health, etc., as well as time-scales of the decision process for humans versus computers. Moreover, the increase of automation in human driven cars can be used to launch cyber attacks that exploit a car's behavior, as perceived by a driver, and the actual behavior as dictated by automation. Therefore new security mechanisms that use the human-in-the-loop in conjunction with automation (at different time-scales) would need to be designed.

Research challenges

As observed above, to secure transportation system requires a holistic approach which combines security of cyber and physical components. Building on this we put forth the following research challenges.

- How to model the interaction and dynamics of the cyber and physical components of a complex transportation system? This is challenging since it involves multiple physical and cyber systems operating and connected in complex topologies.
- How to analyze the security vulnerabilities of such systems? For this intimate domain-specific knowledge is needed, not just of the system behavior but also of the software implementations.
- How to utilize the inter-dependencies to enable secure and robust operation and also enabling countermeasures to attacks?
- How to model and use the "human-in-the-loop" for transportation security?
- How to scale such security to large scale (autonomous) transportation systems?

References

[1] "Google driverless car," See for example New York Times article "Google Cars Drive Themselves, in Traffic, " October 9 2010.

[2] "CMU's Autonomous Cadillac SRX," See http://rtml.ece.cmu.edu/Shuster/

[3] "Car hacking: The next global cybercrime?" CNBC news, See http://www.cnbc.com/id/101123279

[4] "PATH project", See: http://www.path.berkeley.edu/

[5] "Car hacking code released at Defcon," See CNET article August 2013.

[6] "Engineers Hack Traffic Signals in Los Angeles," NBC news, See http://www.nbclosangeles.com/news/local/City-Sees-Red-After-Engineers-Hack-Traffic-Signals–78245117.html

[7] H. Fawzi, P. Tabuada and S N. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," http://arxiv.org/abs/1205.5073

[8] Y. Shoukry, P. Martin, P. Tabuada, M B. Srivastava, " Non-invasive Spoofing Attacks for Anti-lock Braking Systems," CHES 2013: 55-72.

[9] "Foundations of Secure Cyber Physical Systems", NSF project # 1136174, 2011-2015.

[10] A. A. Cardenas, S. Aminy, B. Sinopoliz, A. Giani, A. Perrigz, and S. Sastry. Challenges for securing cyber physical systems. In *Workshop on Future Directions in Cyber-physical Systems Security, DHS*, 2009.