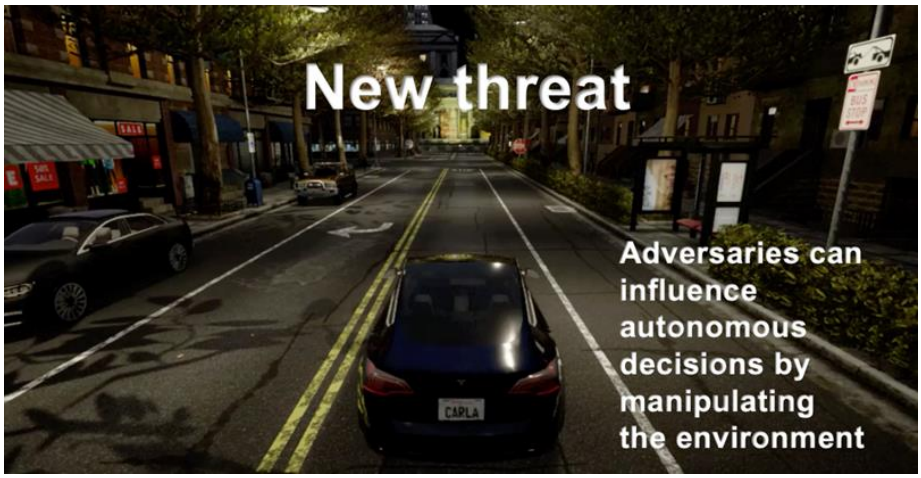
Evaluating Assurance of Autonomous Vehicles

Robots are increasingly playing an important role in applications ranging from manufacturing and construction to surgical robotics. Due to the critical nature of many applications, it is important for the industry to accelerate developing solutions and good practices that address cybersecurity for robotics.



The Cybersecurity for Robotics (CSfR) Conference on December 17-18 played an important role in raising awareness and fostering the growth of a community among researchers, system integrators, business owners, and other key stakeholders. A main theme highlighted challenges existing from different perspectives and across multiple application domains, such as healthcare and autonomous driving. With outstanding technical presentations, the community reaffirmed the urgency of investing in efforts to secure robots.

Through a connection made by MassRobotics and MITRE's Bridging Innovation, MITRE's Dr. Andres Molina-Markham gave a talk and served as a panelist. Andres, a cybersecurity researcher leading two projects under the umbrella of Trustworthy Autonomy at MITRE, outlined several important challenges for evaluating the assurance of autonomous vehicles.

First, he highlighted the threat of perception attacks to safe autonomous driving by pointing out that research over the last few years has demonstrated the feasibility of attacks to camera-based object detectors, LiDAR-based object detectors, and satellite-based positioning systems. Andres argued that while it may take years to see wide deployments of fully autonomous vehicles, Automated Driving Systems (ADS) are increasingly integrating autonomous features with unknown performance in adversarial scenarios.

Andres explained that MITRE is developing a principled approach to address the problem of evaluating the assurance of an ADS when subject to adversarial scenarios. He emphasized important technical problems, including the need for the right formal framework to specify models, with a corresponding computing approach to turn models into evaluation tools. Andres noted that evaluating a single protection mechanism is hard but evaluating systems that integrate multiple protection mechanisms against multiple potential threats is even more challenging.

After illustrating the key issues with examples, Andres concluded by briefly describing a few of MITRE's goals for this research and invited the community to collaborate in solving this important problem. In

particular, Andres noted that applications for MITRE's framework include platform assessments to help ADS developers integrate AI-protection mechanisms in their designs, along with the development of near real-time monitors for autonomy degradation and defense maneuvering when the autonomous vehicle is subject to AI-targeted attacks.

During the panel discussion, panelists reiterated that there are many challenges of increasing autonomy levels in robotic applications. One of the challenges that Andres noted is that in many scenarios, autonomous agents need to operate in a shared environment with multiple agents, some of which may exhibit adversarial behavior. Therefore, while some of the challenges will be related to traditional security problems (e.g., secure communications and access control), others will require novel approaches that take the dynamics of competing agents into account.

When new technologies are introduced, new threats arise. As autonomous systems expand across many domains, Andres and his colleagues at MITRE are partnering across the research community pioneering new methods to counter these emerging threats and make the world safer.