DEPARTMENT OF COMPUTER SCIENCE

TEXAS TECH
Whitacre College of Engineering

Stealthy Attacks on Autonomous Systems

Sibin Mohan, Ph.D.
George Washington University
Tuesday, September 24, 2024
3:30 p.m.
Zoom

Abstract: Autonomous Systems (AVs) require accurate sensing and modeling of the real world in order to carry out their missions. They use the observations from sensors to reason about the vehicle's state and can correct for deviations, even attacks. In practice, even the most meticulously designed control systems always operate under a certain amount of noise because of the unavoidable errors involved in both sensor measurement as well as the modeling of complex vehicular dynamics.

All of this inherently creates a space that can be exploited by an adversary. In this talk, I will present novel methods that can exploit this space, using a software-only attack. Our system, Requiem, presents a blackbox attack -— i.e., there is no knowledge required about the internal details of the system —- the only requirement is that the state estimation function be "learnable" from observation of the inputs and outputs. The final result of a Requiem-based attack causes significant deviations in the physical system's trajectory (sometimes by tens or hundreds of metres!). Meanwhile the system believes it is following the original mission parameters. Hence, this is an attack that is hard to detect or defend against.

Bio: Sibin Mohan is an Associate Professor in the Department of Computer Science at The George Washington University. He also holds an adjunct faculty appointment in the Dept. of Computer Science at the University of Illinois at Urbana-Champaign. Sibin completed his Ph.D. and M.S. in Computer Science from North Carolina State University. His undergraduate degree was in Computer Science and Engineering from Bangalore University, India. In the past, he worked at Hewlett Packard. His research has won multiple best paper awards and he is the recipient of the NSF CAREER award. Sibin's research interests are in the area of systems, security, networking and autonomous systems. Sibin has pioneered research to improve the resiliency and security of real-time, cyber-physical and autonomous systems. Current research efforts include resiliency and security for autonomous and cyber-physical style systems, securing operating systems via code debloating, resiliency for safety-critical networks, security for V2X systems and understanding the behavior of UAV swarms.