UNCONVENTIONAL EXPLOITS IN THE INTERNET OF THINGS

ABSTRACT: The widespread and increasing prevalence of networked devices opens new paths of attack, creating new security challenges. Some of these challenges are conventional cyber-security issues, exacerbated by the much larger and more diverse network now available. Others involve attacks that exploit the interface between cyber and physical domains, for example using physical means to exfiltrate data stored on computer systems, or using network access to physical controls to manipulate or damage physical systems. In this talk, I will discuss the range of these challenges and some workable methods to mitigate them. I will also present research performed at Adventium on using AI planning techniques to explore the range of possible cyber/physical exploits for a moderately complex device.

BIO: Dr. Mark Boddy is Chief Scientist and co-owner of Adventium Labs. His areas of expertise include constraint satisfaction, heuristic search, mathematical optimization, classical planning and extensions thereto, temporal reasoning, multi-agent cooperative negotiation, and resource-bounded reasoning. He co-authored the papers that coined the widely-used terms “anytime algorithm,” “performance profile,” and “conformant planning.” Dr. Boddy’s current and recently-led projects span a wide range of technical areas: building complex mission and planning models to hypothesize exploits on embedded systems; applying constraint-based methods to increase the mission resilience of cloud-based computing; resource allocation and design for modern avionics systems; automated checking of procedures against doctrinal and safety constraints; model integration and meta-modeling for the design of complex cyber-physical systems; and task coordination in decentralized networking applications.