VirginiaTech

VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY

Computer Science Seminar Series

National Capital Region

No Ill Intent? Understanding the Security Threats and Challenges of Intent-Based Networking

Speaker: Prof. Benjamin E. Ujcich
Georgetown University
Friday, February 2, 2024
11:15AM- 12:15PM, NVC 213

Abstract

Traditional computer networks have often relied on manual, static configurations, which have become impractical as networks have grown in complexity. Software-defined networking (SDN) emerged as a solution, separating control and data planes, yet it still required network operators to understand low-level details. Today, intent-based networking (IBN) represents the next evolution in abstracting network complexity by enabling operators to specify "what" the network should achieve through intents rather than "how" such low-level configuration, protocol, and topology details should be managed. This paradigm shift has gained recent traction in practice, adopted by major vendors like Cisco and Juniper, and deployed in large-scale networks such as Google's Orion control plane. Despite IBN's operational benefits, little attention has been paid to the security, trust, and privacy threats and challenges that arise from this shift.

In this talk, I highlight IBN's unique security threats and challenges compared to traditional networks and SDN, and I explore possible strategies to build better and more secure IBN systems. I introduce one strategy for efficiently uncovering exploitable vulnerabilities in IBN implementations with recent work on the Intender project (USENIX Security '23), the first semantically-aware fuzzing framework for IBN. Intender leverages network topology information and intent-operation dependencies to efficiently generate testing inputs. Intender also introduces a new fuzzing feedback mechanism, intent-state transition guidance, which traces the history of transitions in intent states. Intender uncovered 12 bugs in open-source IBN implementations, 11 of which were CVE-assigned security-critical vulnerabilities affecting network-wide control plane integrity and availability.

Biography

Benjamin E. Ujcich is an Assistant Professor in the Department of Computer Science at Georgetown University. His research interests span the secure design of systems and networks, particularly the security of programmable networking architectures. His most recent research has focused on programmable data planes, intent-based networking, and network operating systems. His work has appeared at top security conference venues such as IEEE S&P (Oakland), USENIX Security, Internet Society NDSS, and ACM CCS. He received his Ph.D. in Electrical and Computer Engineering at the University of Illinois at Urbana-Champaign in 2020, where he was co-advised by Adam Bates and William H. Sanders.