COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

# DISSERTATION DEFENSE

## Ramakrishnan Sundara Raman

## Global and Longitudinal Investigation of Network Connection Tampering

Monday, May 6, 2024
11:00am – 1:00pm
3725 Beyster
Hybrid – Zoom

**ABSTRACT:** As the Internet's user base and criticality of online services continue to expand daily, nation-state adversaries like Internet censors are increasingly monitoring and restricting Internet traffic. These adversaries perform large-scale *connection tampering attacks* seeking to prevent users from accessing specific online content, compromising Internet availability and integrity. The community's understanding of the current state and global scope of such connection tampering attacks remains limited: most work has focused on the practices in particular regions or networks at specific points in time, or on the reachability and security of limited sets of online services. Creating a *global, longitudinal, and data-driven* view of connection tampering is an extremely challenging proposition, since such practices are intentionally opaque and tampering mechanisms may vary. Moreover, advances in network technology and recurring instances of tampering events all over the world have necessitated high-quality measurement tools and data that can help researchers, journalists, policymakers, and advocacy groups characterize tampering technology and ensure accountability.

I argue the following thesis: *Connection tampering attacks such as Internet censorship are pervasive, evolving phenomena that need to be studied globally and longitudinally through data-driven network measurements.* To evaluate this thesis, I present a range of empirical methods to longitudinally investigate connection tampering at the global scale. First, I explore the development of a global, longitudinal censorship measurement platform, the Censored Planet Observatory, that uses remote measurement techniques to safely measure Internet censorship in more than 200 countries. Censored Planet has collected more than 65 billion measurement data since 2018, and I overcome key challenges in the analysis of large-scale censorship measurement data. Next, I present novel measurement methods to investigate the network technology that enables connection tampering, and propose frameworks to monitor their deployment around the world. I also advance methods to rapidly measure evolving tampering attacks with new threat models, such as the large-scale HTTPS interception attack in Kazakhstan in 2019. Finally, I envision intelligent censorship measurement platforms that optimize censorship measurements through reinforcement learning. My research collectively demonstrates that Internet censorship and large-scale tampering attacks consistently present new threat models, impacting a large segment of the Internet globally.new threat models, impacting a large segment of the Internet globally.

**CHAIR:** Prof. Roya Ensafi