Abstract: Over the last decade, my research group has extensively studied Internet threats: the nature of botnets, worms, denial-of-service, and a wide range of malware. While there’s much to learn from this attack-centric viewpoint, in recent work we have focused on understanding the threat landscape through the role of networks themselves.

In this talk, I will highlight a recent series of work in which we measure and model how networks, suitably defined, influence and are influenced by malicious behavior on the Internet. Through analysis of Internet-scale observations, we show that networks’ observed maliciousness is strongly correlated with spatial distance, that aggregate maliciousness evolves over time in predictable ways, and that the dynamics of this evolution can serve as a proxy for understanding the overall security hygiene and responsiveness of each network. Taken together, these observations lead to models of network maliciousness that can inform strategies for improving the overall health of the Internet. Applying these models, we explore a policy that seeks to quarantine the carriers of harmful traffic, and analyze the tradeoffs between improvements in security, stability, and performance versus losses in important core Internet properties that would ensue from actively disconnecting the most egregiously malicious networks.

Short Bio: Michael Bailey is Research Associate Professor and Co-Director of the Network and Security Research Group at the University of Michigan. His research is focused on the security and availability of complex distributed systems. Prior to his appointment at the University of Michigan, he was the Director of Engineering Arbor Networks, a Lecturer at DePaul University, and a Programmer/Analyst at Amoco corporation. He was awarded the College of Engineering Kenneth M. Reese Outstanding Research Scientist Award in 2011, the University of Michigan Research Faculty Recognition Award in 2012, and was elevated to senior member of IEEE in 2009 and senior member of ACM in 2013. Michael received his PhD in Computer Science and Engineering from the University of Michigan in 2006.