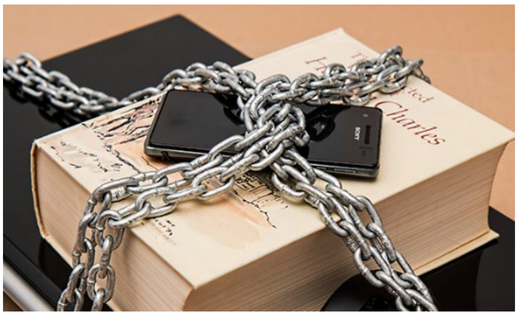

Security Lancaster | Lancaster University

Institute Seminar

The Curse of Learning and Extracting Fast-Evolving Cyberattack Behaviors

Professor Shanchieh Yang
Rochester Institute of Technology

Date: May 28th, 2021
Time: 14:00-15:00
Teams Link: Join Seminar (We'd appreciate if you could optionally register to join our mailing list)

Abstract:

Critical and sophisticated cyberattacks often take multitudes of reconnaissance, exploitations, and obfuscation techniques to penetrate through well protected enterprise networks. As both attack behaviors and networked systems continue to evolve, in an ever-increasing speed, traditional cybersecurity research and practices suffer from catching up to the changes. Successes in artificial intelligence and machine learning has pushed research to detect, prevent, and predict cyberattacks based on labeled datasets. Unfortunately, labeled data is almost always guaranteed to be either outdated or non-transferable. This talks will discuss the limitations of applying traditional approaches as well as research advances that tackles the fast-evolving nature of cyberattacks. Specifically, we will show examples that fail to recognizing evolving cyberattacks and some of the novel ideas to tackle this problem. We will also demonstrate a research prototype system – ASSERT – on how it continuous to learn and adapt in near real-time and without any labeled data. We will discuss with the audience on future research directions and how security practitioners may use and trust systems that do not have labeled data to verify their performance.

Biography:

S. Jay Yang received his MS and Ph.D. degrees in Electrical and Computer Engineering from the University of Texas at Austin in 1998 and 2001, respectively. He is currently a Professor in the Department of Computer Engineering and Director of Global Outreach for Global Cybersecurity Institute at Rochester Institute of Technology. Supported by NSF, NSA, IARPA, DARPA, AFRL, ONR, and ARL, his research team has developed several pioneering machine learning, attack modeling, and simulation systems to enhance cyber situational awareness and enable anticipatory cyber defense. His earlier works included FuSIA, VTAC, ViSAw, F-VLMM, and attack obfuscation modeling. His recent works include ASSERT to employ information theoretic unsupervised learning to provide timely generation and synthesis of attack models, CASCASE to simulate cyberattack scenarios by integrating data-driven and theoretically grounded understanding of adversary behaviors, and CAPTURE to forecast cyberattacks before they happen using unconventional signals from the open sources. He was a NSF Trusted CI Open Science Fellow in 2019 and TTP Fellow in 2020, and received IEEE Region 1 Outstanding Teaching in an IEEE Area of Interest Award – for outstanding leadership and contributions to cybersecurity and computer engineering education. Over the past 10 years, he has also established several international partnership programs with universities in United Kingdom, Czech Republic, Poland, Ireland, Netherlands, Germany, Taiwan, Japan, and South Korea.

Please contact Jennifer for any Teams connectivity issues: j.mcculloch@lancaster.ac.uk