ILLINOIS ARCS ADVANCED RESEARCH CENTER AT SINGAPORE

TSCP-DC | TRUSTWORTHY AND SECURE CYBER-PLEXUS FOR DIGITAL COMMUNITIES

illinois-arcs.edu.sg/

THRUST 4
EVALUATION

Validating core security capabilities by developing robust evaluation methods for new technologies to evaluate risk, resilience, and asset criticality within real-world digital infrastructures.

The first three thrusts (Cyber-Plexus System Protection, Trust Assurance, and Cyber-Plexus System Analysis) focus on building the core capabilities needed to develop trustworthy, secure systems for digital communities. The Evaluation thrust builds on this foundation by providing the infrastructure and means to evaluate these capabilities in realistic operational environments.

Evaluation is critical because digital communities comprise highly interconnected subsystems with complex dependencies. Interactions across components can produce behaviors that are difficult to predict during operations. Evaluating technologies in realistic settings enables researchers to validate effectiveness, identify unintended consequences, and understand system-level impacts before deployment. It also ensures that security solutions remain robust under real-world conditions, where scale, heterogeneity, and operational constraints introduce additional challenges.

The Evaluation thrust advances this vision by bringing together two complementary efforts.

1. **A living lab security architecture for evaluating technologies safely, realistically, and at system scale**
2. **Methods for evaluating the security of digital communities through continuous monitoring, distributed data collection, and vulnerability assessment.**

The three core capabilities developed in this thrusts are:

1. **A scalable security monitoring platform that provides real-time visibility into network activity, device vulnerabilities, and potential attack paths, enabling informed and timely operational decisions.**
2. **A Graph Convolutional Network (GCN)-based method integrated with real-time monitoring to identify and rank critical assets whose compromise could have the greatest impact on the wider system.**
3. **An adaptive anomaly detection approach that combines Temporal Convolutional Networks (TCNs) with variational autoencoders (VAEs) to distinguish between normal operational drift and malicious activity, allowing the system to adapt while maintaining resilience.**

Meet the Team

Zbigniew Kalbarczyk, Ph.D.
Professor, Coordinated Science Laboratory,
University of Illinois Urbana-Champaign

Aditya Mathur, Ph.D.
Professor; Founding Centre Director, iTrust,
Singapore University of Technology and Design

Steven Wong, Ph.D.
Professor; Director, Centre for Digital Enablement (CoDE),
Singapore Institute of Technology (SIT)

Heng Chuan Tan, Ph.D.
Senior Research Scientist,
Illinois Advanced Research Center at Singapore

Le Ly Tu Tran (Fiona), Ph.D.
Postdoctoral Researcher,
Illinois Advanced Research Center at Singapore