ILLINOIS ARCS ADVANCED RESEARCH CENTER AT SINGAPORE

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

illinois-arcs.edu.sg/

THRUST 3
CYBER-PLEXUS SYSTEM ANALYSIS

Developing sophisticated modeling techniques and frameworks to capture complex behaviors and evolutionary patterns of the cyber-plexus system in response to the diverse triggering events within the digital communities.

The Cyber-Plexus System Analysis thrust is built upon developing specialized models that map out the digital landscape of smart communities and scalable algorithms that perform security analysis for the protection of those communities.

The thrust aims to build a framework that is capable of capturing the behavior of the digital community network, and analyzing it for trends, patterns, and relationships within the data in order to facilitate analysis of the network's security. The framework can then be used as an experimental virtual testbed to test security solutions, threats, and glitches.

Key Objectives

To evaluate cyber-security resilience by analyzing and predicting the behavior of the system under cyber security threats. The focus is on developing modeling techniques that capture the impact of actions, such as attacks and network changes, on large system-of-systems.

- **Analyze how the system responds to malicious actions**
- **Determine the expected behavior of the system under both normal and abnormal operation scenarios**
- **Measure the impact of deploying security solutions on the performance of the system**

The Challenge

Establishing a reliable digital twin requires reconciling discrepancies between different sources of information at varying levels of granularity, detail, and accuracy. Such significant challenges arise due to the lack of visibility into the system, up-to-date structured documentation, and understanding of the system context. Thus, there is a need to address the diverse sources of data to ensure that the subsequent analyses are based on trusted models.

The Solution

The Cyber-Plexus Systems Analysis thrust resolves this challenge by designing advanced multi-resolution models that simulate system behavior and realistic and evolving threats. The main research outcome is establishing a methodology to gather digital community data into analyzable models that evaluate the cyber-plexus's fundamental state and behaviors. By modeling how security solutions and attacks influence the behavior of cyber-plexus, the resulting framework identifies gaps in the security of the system.

Meet the Team

David M. Nicol, Ph.D.
Director of Research (Cyber); Herman M. Dieckamp Endowed Chair in Engineering; Director, Information Trust Institute, University of Illinois Urbana-Champaign

David Yau, Ph.D.
Professor, Information Systems Technology and Design (ISTD), Singapore University of Technology and Design

Malcolm Low, Ph.D.
Associate Professor,
Singapore Institute of Technology (SIT)

Carmen Cheh, Ph.D.
Senior Research Scientist,
Illinois Advanced Research Center at Singapore