ILLINOIS ARCS ADVANCED RESEARCH CENTER AT SINGAPORE

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

illinois-arcs.edu.sg/

THRUST 2
TRUST ASSURANCE

Designing system architecture to bridge the gap between theoretical design and practical deployment by automating policy generation tool and network verification system to ensure scalable, verifiable security across complex digital infrastructures.

Developing tools and applications to measure the effectiveness of security controls in improving trustworthiness is the core focus of the Trust Assurance thrust. While tools such as formal methods, mathematics, and algorithms provide foundational guarantees for systems and controls designs, these design assurances are not sufficient. It is essential to have practical implementations of these designs to be verified as trustworthy.

Vulnerabilities, configuration oversights, and systemic weaknesses often arise from gaps between design and deployment; this thrust therefore emphasizes policy formulation and automated policy generation, complemented by formally verifiable networking that enables trustworthy path validation, scalable network-wide verification, and reliable intent-to-policy translation to strengthen cybersecurity protections for digital communities.

The Challenge

The cyber plexus is a non-conventional large-scale system. It comprises complex and programmable components involving cooperation and competition among multiple stakeholders. While robust formal methods, such as the mathematical approach, synthesize physical and computational components through symbolic logics, it struggles to scale within this complexity, and operators often lack training in formal logics.

Provide assurance for security policies that are derived from observation of system behaviors and knowledge of system structures, including validation of meshes of independently developed and interacting policies.

-Develop policies where multiple independent policy developers and enforcers are within the core-and-tenants architecture, as well as ensure the security of networks used for system observations.

The Solution

The Trust Assurance thrust builds upon the automated generation of security policies through an initial three-phase process: defining generic policy templates, associated keywords in the templates with the system data, and generating the policy enforcement code in the machine syntax.

Earlier research established a foundational structure for policy templates but lacked the proof of assurance needed to guarantee policy coverage and correctness. To address this, the security policy framework utilizes statistical analysis to infer invariants from data traces to identify properties that the automatically generated security policies must assure. The framework also needs to account for the impact of noise in data on the policy.

If clarity is needed on firewall rules, the TSCP appliance, featuring an intuitive chat-based support system allows simple conversations in plain English to facilitate understanding of network architecture structure, or request the AI framework to automatically draft and apply robust policies. Enterprise-level protection can be achieved without network or security expertise.

This thrust aims to deliver a practical device authentication solution that is suitable for adoption and application by the stakeholders in digital communities. With the implementation of the novel tool, the framework addresses established challenges regarding computation and storage complexities. This approach will facilitate platform scalability that enhances standardization of distributed trust architectures for digital communities.

Meet the Team

Matthew Caesar, Ph.D.
Professor, Siebel School of Computing and Data Science,
University of Illinois Urbana-Champaign

Binbin Chen, Ph.D.
Associate Professor; Associate Head of Pillar (Innovation and Enterprise),
Singapore University of Technology and Design

David Sanan, Ph.D.
Associate Professor, Programme Leader,
Singapore Institute of Technology (SIT)

Ertem Esiner, Ph.D.
Lead Research Scientist,
Illinois Advanced Research Center at Singapore

Xenia Santos, Ph.D.
Postdoctoral Researcher,
Illinois Advanced Research Center at Singapore

Kulani Mahadewa, Ph.D.
Postdoctoral Researcher,
Illinois Advanced Research Center at Singapore