ILLINOIS ARCS ADVANCED RESEARCH CENTER AT SINGAPORE

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

illinois-arcs.edu.sg/

THRUST 1
CYBER-PLEXUS PROTECTION

Engineering robust AI-driven defense and AI-resilient systems within high-performance environments to detect complex evolving threats while mitigating infrastructure risks in operational computing environments.

The Cyber-Plexus Protection thrust focuses on technologies to secure the digital community's interconnected infrastructure, specifically prioritizing AI-driven defense and the establishment of AI-resilient systems. This work builds upon prior research involving anomaly detection in power systems. Current efforts balance the development of advanced AI models for sophisticated attack detection and protection with the engineering of hardware systems designed to make these solutions deployable and practical in real-world scenarios.

While AI-based solutions offer high detection accuracy, the research simultaneously addresses critical implementation challenges, alongside primary initiatives focused on predictive hardening and AI models designed for complex, evolving threat vectors. To mitigate scalability constraints, the thrust proposes a unified high-performance system designed for low false-alarm rates and rapid response times within high-performance computing environments.

The Challenge

Digital communities integrate diverse platforms (HVAC systems, smart grids, and autonomous vehicles) into a shared infrastructure. Establishing trust across these platforms is complicated by inconsistent security requirements and complex cross-platform topologies. Key challenges include:

Sophisticated Threat Landscape:
Traditional defenses struggle against stealthy APTs and Zero-Day vulnerabilities that have no known signatures.

Absence of Unified Trust:
Independent platforms lack inherent trust relationships, making cross-platform coordination vulnerable to identity spoofing.

Heterogeneous & Dynamic Environments:
The network must support both high-performance nodes and resource-constrained devices that frequently join or leave, rendering traditional certificate management inefficient.

Performance Constraints:
Security must not compromise responsiveness; detection mechanisms must meet strict real-time latency requirements to protect critical urban services.

The Solution

Thrust 1 implements a multi-layered security architecture that balances high-accuracy AI-driven solutions with hardware-speed verification and implementation:

1. **iPROTECT (AI-Based Protection):** An AI framework designed to detect and protect against advanced threats, including Zero-Day and supply-chain attacks. It has demonstrated over 98.0% detection accuracy in fine-grained detection across diverse DDoS attacks.

2. **Hardware-Accelerated Protection (SecureMPV):** A provenance-aware verification system implemented on programmable hardware and DPUs. It achieves microsecond-level latency (~2.9 µs in switch environments and ~40 µs on DPUs), enabling the real-time detection of policy violations and tampering.

3. **Privacy-Preserving Computation (MPC):** A novel hardware-software co-design for Multi-Party Computation that achieves a 6.8× speedup over conventional GPU-based solutions, allowing secure collaboration across different administrative domains.

4. **Distributed Trust Framework:** A permissioned distributed architecture utilizing blockchain principles and digital signatures to facilitate secure device authentication and establish trust among verified participants.

Meet the Team

Deming Chen, Ph.D.
Professor, Co-Director, IBM-Illinois Discovery, Accelerator Institute

Jianying Zhou, Ph.D.
Centre Director, iTrust, Professor, Singapore University of Technology and Design

Weihan Goh, Ph.D.
Associate Professor, Singapore Institute of Technology (SIT)

Muhammad M. Roomi, 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