CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Nasir Memon, PI

Quanyan Zhu, co-PI

Junaid Farooq, RA

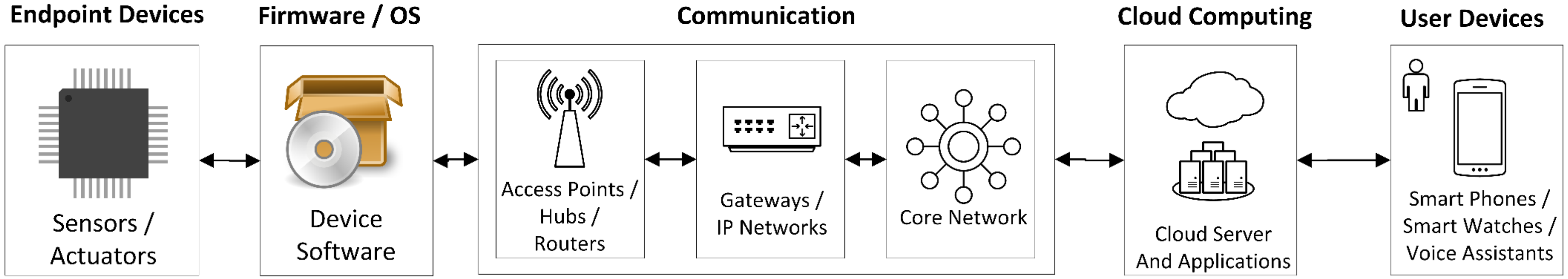
NEW YORK UNIVERSITY

Multi-Layer Cyber-Physical Supply Chain Risk Analysis for Improving the Resilience of IoT-Enabled Critical Infrastructures

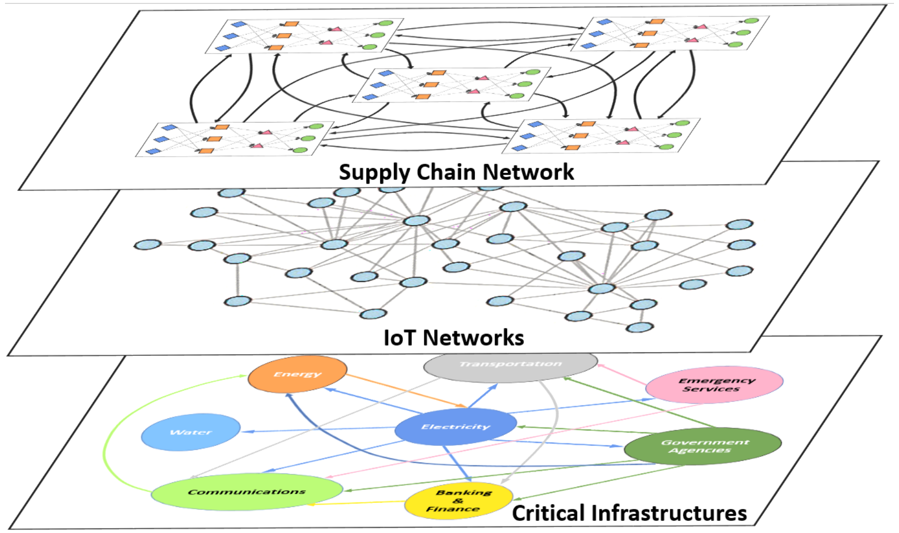
Apr. 11, 2019

Introduction

- The widespread adoption of the IoT is becoming indispensable in the nation's critical infrastructure systems such as in energy, transportation, communications, emergency services, public administration, defense, etc.
- The IoT is not a standalone system obtained from a single supplier/manufacturer. Instead, it is an interconnection of multiple hardware and software systems manufactured by different entities located in different parts of the world.



Introduction



- The integration of multiple components manufactured and designed separately results in enhanced vulnerability of the underlying critical infrastructure to cyber-physical attacks.
- The interconnection of IoT systems and infrastructure leads to a complex web of suppliers, manufacturers, and service providers.

Research Questions

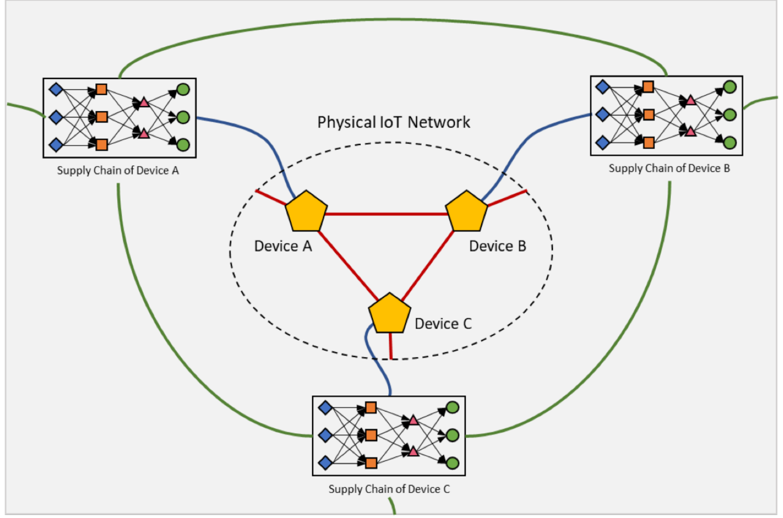
- What are the potential sources of attack in an IoT ecosystem from a supply chain perspective?
- How to model and understand the complex web of supply chain actors underlying the IoT enabled critical infrastructures?
- How to analyze the multi-layer propagation of cyber-physical threats that emanate from the IoT supply chain?
- How to develop integrated decision support tools to enable risk mitigating IoT network deployment and procurement decisions?

Research Objectives

- Creating a **scalable mapping** of the threat actors in the supply chain of IoT devices and networks.
- Development of **multi-layer network models** to capture hidden supply chain linkages in IoT-Enabled CI for a holistic risk analysis across different sectors.
- Development of **systematic approaches** to IoT supply chain risk analysis and propagation.
- Development of **integrated decision analytic tools** that assist in making risk mitigating decisions at the procurement, deployment, and upgrade phases.

Approach

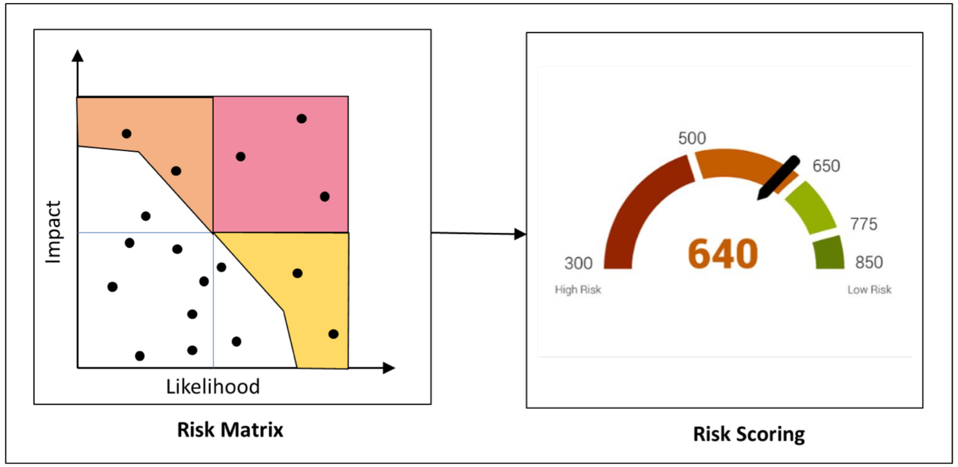
1. Mapping Threat Actors in the Supply Chain Network of IoT-Enabled Infrastructures
   - Identification, Categorization, and Mapping of Threat Actors & Attack Surfaces
   - Multi-Layer Network Modeling of IoT and Underlying Supply Chain Networks



Approach

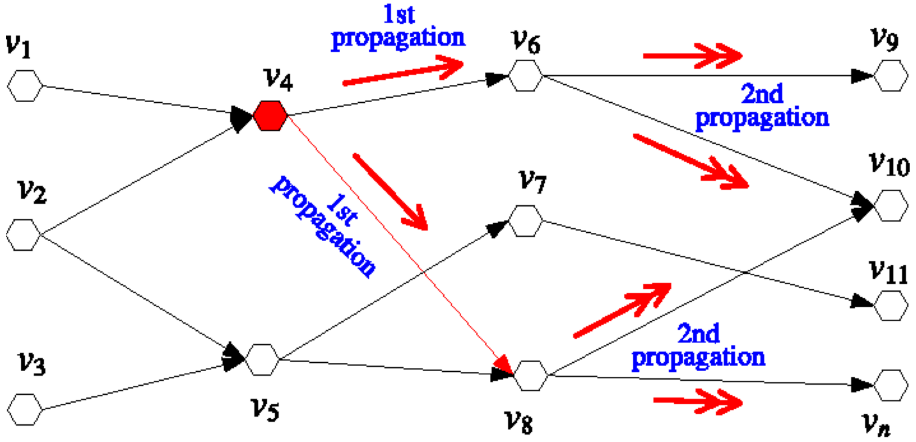
2. Cyber-Physical Supply Chain Risk Assessment in IoT-Enabled Critical Infrastructures

- Systemic Vulnerability Assessment of Supply Chain Oriented Risks
- Analysis of Risk Propagation via Multi-Layer Cyber-Physical Supply Chain Network



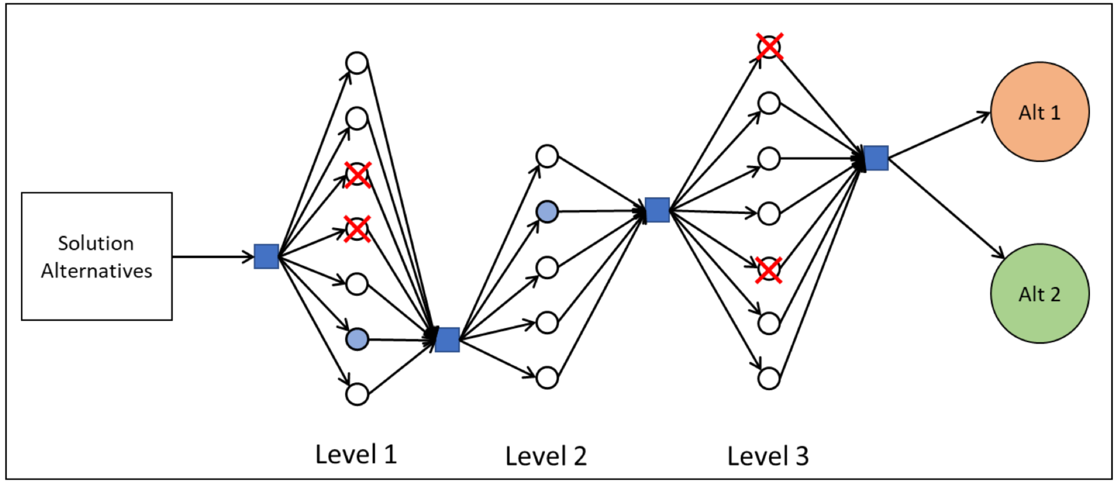
Risk Matrix

Risk Scoring



Approach

3. Decision Support Tools to Improve the Resilience of IoT-Enabled Infrastructures
   - Decision Analytics for Procurement, Deployment, and Upgrade of IoT-Enabled Infrastructures
   - Development of Large Scale Multi-level Risk Mitigation Strategies



Outreach and End User Engagement

- This research will disseminate results to affiliates of **NYU Center for Cyber Security (CCS)** and **Cyber Security Awareness Week (CSAW)**.
- This project will engage researchers from **Tag-Cyber** and **Siemens Research**.
- This research will organize an IoT security meeting with industry partners and stakeholders in June.

Benefits to DHS/HSE

- Tools and methods to **analyze** cyber-physical risk in existing IoT-enabled CI.
- Assist in making risk informed decisions on **procurement**, **deployment** and **operation** of IoT-enabled critical infrastructure.
- Assist in developing cyber security **recommendations**, **regulations**, and **policies** for enterprises that manage IoT-enabled critical infrastructure.

Contact

- Nasir Memon, Email: nm1214@nyu.edu
- Quanyan Zhu, Email: qz494@nyu.edu
- Junaid Farooq, Email: mjf514@nyu.edu