CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Cybersecurity Assurance for Critical Infrastructure

Jason Jaskolka
Carleton University

Project Overview

Develop an improved understanding of the increasingly distributed, complex, and richly connected critical infrastructure environment at a systems level to provide valuable insights into improving security and resilience

- Advance ***cybersecurity assurance*** by providing valuable and insightful information regarding:
  - Mitigating the vulnerabilities and risks introduced by the existence of implicit interactions
    - ***Implicit interactions:*** component interactions within a distributed system that may be unfamiliar, unplanned, or unexpected, and either not visible or not immediately comprehensible to the system designers
  - Reducing the impact when a system experiences an attack or failure
  - Making it more practical to address cybersecurity early in system development
  - Design, implementation, and cyber-assurance decisions, as well as mitigation strategies and policies
- Identify ***strengths and weaknesses*** of the methodology
  - Inform further development and technology transition initiatives

Approach

Modeling and Specification

- Developed a ***formal methods-based approach*** for identifying and analyzing existence of implicit interactions in critical infrastructure systems
  - Involves the specification and analysis of the communication among system components using a mathematical modeling framework known as C^2KA

System Analysis

- Finds the ways in which a compromised system component can cause disruptions to operations by exploiting identified implicit interactions
- Developed a ***software prototype*** to automate the analysis methodology to:
  - ***Identify implicit interactions*** in a given system specification
  - ***Compute the severity and exploitability*** of the identified implicit interactions

Testing, Evaluation, and Validation

- Acquired a real-world case study system of a ***wastewater dechlorination process*** from the SCADA operators at Robert O. Pickard Environmental Centre (ROPEC) within the City of Ottawa
- Shared and presented detailed reports of the methodology and analysis including:
  - Informal system description
  - System specification using the C^2KA modelling framework
  - System analysis results generated by the prototype software tool
- ***Validated*** by the Senior Control Systems Engineer and team responsible for the system
- Administered a ***questionnaire*** to City of Ottawa that was completed by six stakeholders operating at ROPEC
  - Respondents found the approach and results to ***exceed their expectations***
  - Consensus that the analysis results were ***understandable*** and ***valuable*** to their team/organization with the potential to "*identify hidden problems and perhaps provide cost savings and time*"

Milestones and Accomplishments

Outcomes Achieved to Date

1. Approach for identifying implicit interactions
2. Approach for evaluating severity and exploitability of implicit interactions
3. Software prototype for specifying system, and identifying and analyzing implicit interactions
4. Approach for simulating complex systems
5. Validation of the developed approaches with case study applications
6. Dissemination of work through Publications (3) and Presentations (15)

Milestones Remaining

- Transition the developed approaches into practice so that they can be easily adopted and integrated into system development workflows by our end-users and customers

Obstacles/Impediments that Have Been Overcome

- Many potential end-users/customers were unable/unwilling to share descriptions of their systems for the purpose of validating the project results and outcomes due to PI's Canadian citizenship
  - *Mitigation Strategy*: Engaged with Canadian critical infrastructure providers/operators to broaden the scope of the pool of potential end-users

Project Impact

- Addresses the ***need for enhanced understanding*** of **the *linkages between critical system components*** to study the integrity, sustainability, reliability, and vulnerabilities of critical infrastructures
- Capable of providing critical infrastructure ***designers, integrators, owners, and operators*** with actionable information that can drive design, implementation, and cyber-assurance decisions
  - ***Where and how to spend valuable resources*** in mitigating the potential for such attacks on systems
  - Formal foundation upon which mitigation approaches can be developed
  - Basis for ***developing policies and guidelines*** for designing and implementing critical infrastructure systems that are resilient to cyber-threats
- Impact validated through feedback received from SCADA operators at a ***wastewater treatment facility*** where we have applied our research outcomes and approaches
  - Questionnaire results show that performance targets for the developed approach have been meet
    - Consensus that the approaches and results are ***valuable, understandable, and exceeded expectations***
  - Makes it more practical to address cybersecurity early in system development

Transition Plans

- Main output of this research is a ***system-level assessment methodology*** facilitating identification and analysis of cybersecurity vulnerabilities (i.e., implicit interactions) in critical infrastructures
- Methodology has been transitioned to the scientific community in the form of academic publications in ***high-impact technical conferences and journals***
- Plan to transition our developed approaches into ***open source platform*** which involves:
  1. Developing a ***scalable software tool*** that can effectively support the specification of complex systems, as well as to automate the developed vulnerability identification and analysis techniques
     - We currently have a prototype of this software tool that we are using to run our experiments
  2. Working with CIRI leadership in identifying suitable personnel to undertake the software development activities, as well as marketing and business development
- Actively engaging with owners, operators, and integrators of critical infrastructure systems both in industry and in the government sector
  - Current engagement with City of Ottawa's Robert O. Pickard Environmental Centre (ROPEC); conducted a case study system analysis and administered a feedback questionnaire to gauge interest in the project results
  - Plan to work with Illinois Business Consulting Group (IBC) for customer discovery