A Game-Theoretic Intrusion Response and Recovery Engine

Overview and Problem Statement

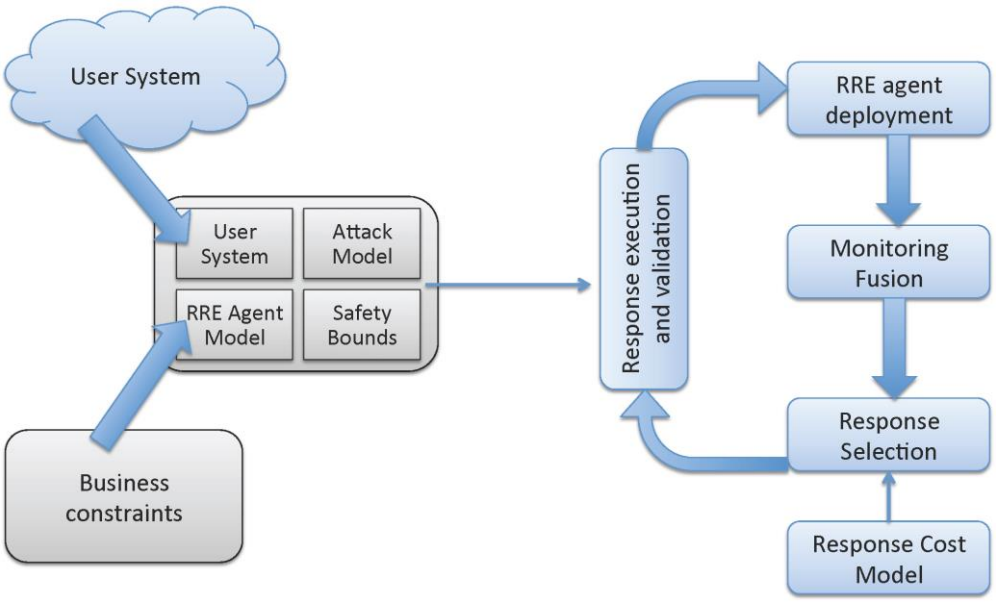
The severity and number of intrusions on computer networks, including networks in electric grids and other critical infrastructures, are rapidly increasing. Preserving the availability and integrity of networked computing systems in the face of those fast-spreading intrusions requires advances not only in detection algorithms, but also in intrusion tolerance and automated response techniques. In this project, we study an intrusion-tolerant system design that can adaptively react against malicious attacks in real-time, given knowledge about the network's topology (determined offline), and alerts and measurements from system-level sensors (gathered online).

Research Objectives

- Develop reactive response against adversarial attacks that uses knowledge about the power grid's current security state and its security requirements.
- Build a Response and Recovery Engine (RRE) as a distributed system that actively monitors systems and devises reactive and proactive responses.
- Use theoretical methods to find optimal response deployment.
- Adapt RRE to handle the scale of a large Advanced Metering Infrastructure (AMI).
- Model the smart grid as a cyber-physical system to study the cyber-physical interactions in detection and response. Interactions include how to detect a cyber attack physically and how a cyber response can help in a physical situation.
- Implement a response and recovery system that is capable of effectively interfacing with a human operator.
- Verify safety of certain responses with respect to system invariants.
- **Smart Grid Application Area:** Intrusion tolerance.

Technical Description and Solution Approach

- Use the cyber-physical topology language (CPTL) as a description of the system. CPTL will be used by RRE agents when computing optimal responses and fusing sensory data.
- Develop monitoring fusion algorithms that can detect high-level attack steps using diverse data sources. The diverse data sources increase confidence that malicious events will be detected.
- Adapt several languages to express the responses in our response taxonomy. RRE agents use the response language to map high-level actions into low-level actions.
- Design several cost-sensitive response selection algorithms based on distributed control theory, game theory, and graph theory.



Results and Benefits

- Distributed intrusion tolerance architecture suitable for the power grid.
- Implementing a basic OpenFlow (software-defined network) responder in a substation setting.
- Advancing the state of CPS modeling.

Researchers

- Ahmed M. Fawaz, afawaz2@illinois.edu
- Robin Berthier, rgb@illinois.edu
- William H. Sanders, whs@illinois.edu

Industry Collaborators

- Schweitzer Engineering Laboratories

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security