Year 2 Activities

(Tasks 2.1 and 2.2)

Hamed Mohsenian-Rad (UCR)
Fabio Pasqualetti (UCR)
Chengyu Song (UCR)

UNIVERSITY OF CALIFORNIA, RIVERSIDE

Physics-Aware Attack Detection

- Lead: Hamed

- Physics-aware methods will help:
  - Monitor state of the health and safety of equipment and physical assets
  - Distinguish natural anomalies from malicious behavior

Physics-Aware Attack Detection

- Lead: Hamed
- Physics-aware methods will help:
  - Monitor state of the health and safety of equipment and physical assets
  - Distinguish natural anomalies from malicious behavior
- Data-Driven Situational Awareness
  - Detection and Classification of Malicous Events
  - Three Classes: 1) Benign, 2) Anomaly, 3) Attack

Physics-Aware Attack Detection

- Lead: Hamed
- Physics-aware methods will help:
  - Monitor state of the health and safety of equipment and physical assets
  - Distinguish natural anomalies from malicious behavior
- Data-Driven Situational Awareness
  - Detection and Classification of Malicous Events
  - Three Classes: 1) Benign, 2) Anomaly, 3) Attack
- Attacks Against Data-Driven Situational Awareness
  - Detection and Identification and False Data Injection Attacks
  - Location Identification, State Estimation, Fault Location, etc.

Automated Firmware Hardening

- Lead: Chengyu
- Investigate new automated binary transformation techniques to provide such patches for grid equipment and resources.

Automated Firmware Hardening

- Lead: Chengyu
- Investigate new automated binary transformation techniques to provide such patches for grid equipment and resources.
- Deploy exploit prevention techniques such as non-executable data, stack canary, address space layout randomization, control-flow integrity, etc.

Automated Firmware Hardening

- Lead: Chengyu
- Investigate new automated binary transformation techniques to provide such patches for grid equipment and resources.
- Deploy exploit prevention techniques such as non-executable data, stack canary, address space layout randomization, control-flow integrity, etc.
- Some devices may not be upgradable. In such cases, we investigate other attack prevention strategies. New firewall filtering rules will be generated and deployed to prevent malicious network communications to/from the device.

Cyber-security Analysis of Interconnected Dynamics

- Lead: Fabio

- The interconnection structure creates new attack surfaces that can be exploited by attackers, may generate instabilities due to feedback loops, and increase the difficulty of isolating corrupted components due to multiple connections.

Cyber-security Analysis of Interconnected Dynamics

- Lead: Fabio
- The interconnection structure creates new attack surfaces that can be exploited by attackers, may generate instabilities due to feedback loops, and increase the difficulty of isolating corrupted components due to multiple connections.
- Challenge: Developing dynamic models for power *distribution* systems.

Cyber-security Analysis of Interconnected Dynamics

- Lead: Fabio
- The interconnection structure creates new attack surfaces that can be exploited by attackers, may generate instabilities due to feedback loops, and increase the difficulty of isolating corrupted components due to multiple connections.
- Challenge: Developing dynamic models for power *distribution* systems.
- Given such models, the knowledge on underlying physics and dynamics of distribution grid interconnections will be used also to reveal cyberattacks that would otherwise remain stealthy locally. This will be done by utilizing our security-aware functional model to check fundamental properties such as controllability, observability, and zero dynamics.