Runtime Semantic Security Analysis to Detect and Mitigate Control-Related Attacks in Power Grids

Challenge:

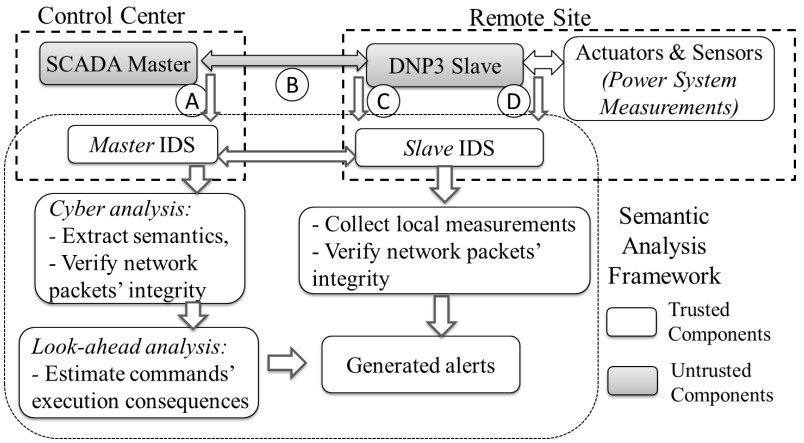
- Control-related attacks:
  - Penetrated isolated control networks
  - Use commands crafted in legitimate formats to cause damage
- Hard to detect control-related attacks
  - Few anomaly activities are found in SCADA networks
  - Few attack signatures are publically available

Scientific Impact:

- Detect attacks by estimating the consequence of executing commands
- Balance detection accuracy and latency
  - Reduce the computation time by fifty percent compared with AC power flow analysis
  - Increase the accuracy by two orders of magnitudes compared with DC power flow analysis

Solution:

- Extend Bro IDS to support protocols in Power Grids
- IDS at control center
  - Use power flow analysis to analyze commands
  - Adapt power flow analysis to balance detection latency and accuracy
- IDS at substations
  - obtain trusted measurements from local sensors
  - Validate absence of corrupted measurements at other locations



Broader Impact:

- Provides protection to manual commands
  - Does not affect the normal operations
  - Can be extended to other industrial control systems
- IDS can be equipped with other scenario-specific policies

Semantic Security Monitoring for Industrial Control Systems, NSF Award #1314891

Contacts: Adam Slagell slagell@illinois.edu (PI), Ravishankar Iyer (Co-PI)