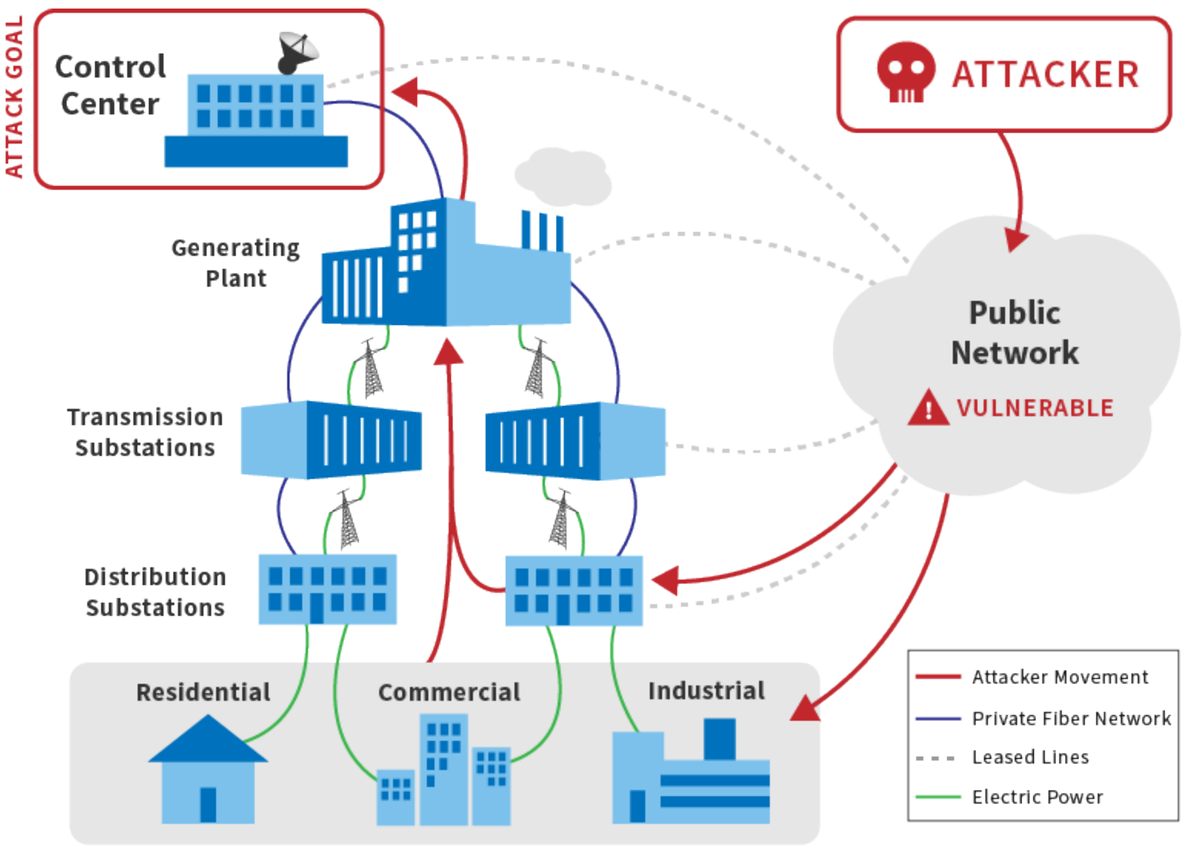
Proactive Response Strategy for Energy Delivery Systems

Mohammad Noureddine, Atul Bohara, Brett Feddersen, William H. Sanders

THE POWER-GRID IS VULNERABLE

- An attack on the US power grid has an estimated cost of $1 trillion to the US economy
- Cyber attack on Ukraine power grid left 225000 users without power

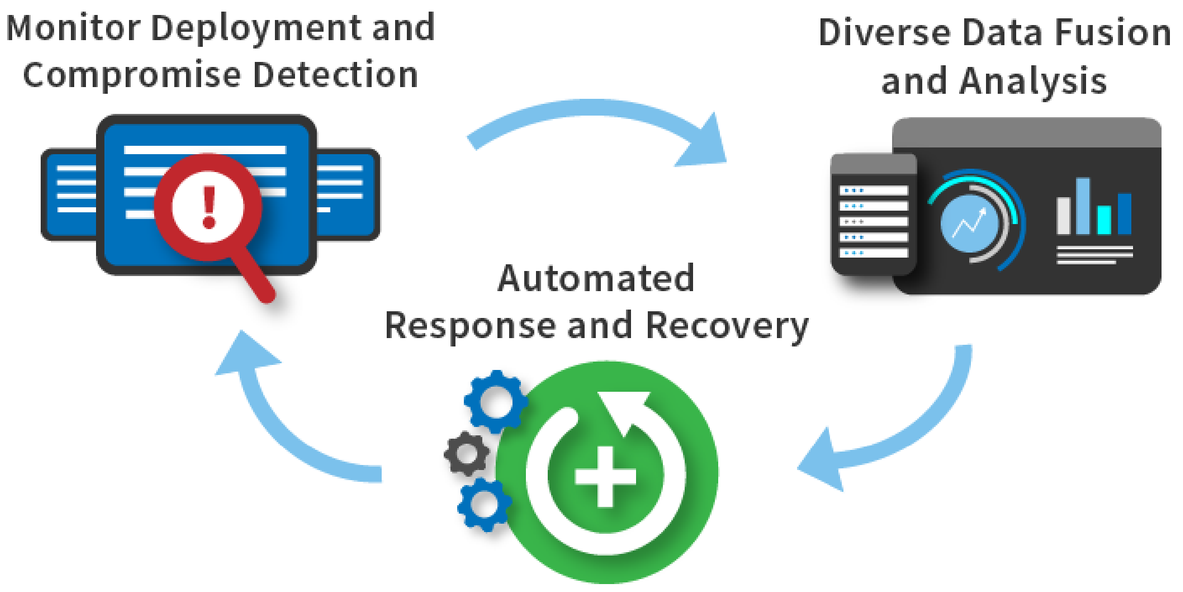


- The power grid is increasingly reliant on its cyber infrastructure for timely and reliable transmission and delivery
- Attackers are employing varied and sophisticated techniques targeting different parts of the grid
  - Denial of Service attacks from the Public Networks
  - Compromise of residential and commercial loads then move into more impactful areas of the network
  - Lateral movement - In the Ukraine incident, attackers spent a significant amount of time moving within the network to reach the control center

RESEARCH VISION

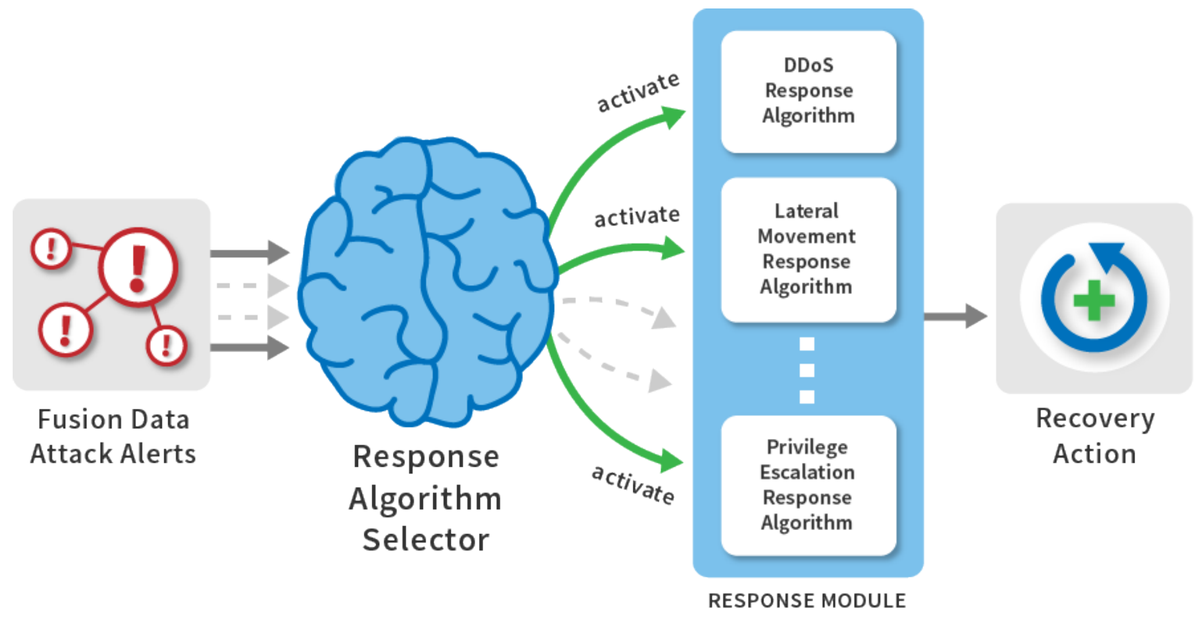
We aim to develop techniques for fast and reliable detection of attacks and effective response through control commands.

RESEARCH ROADMAP



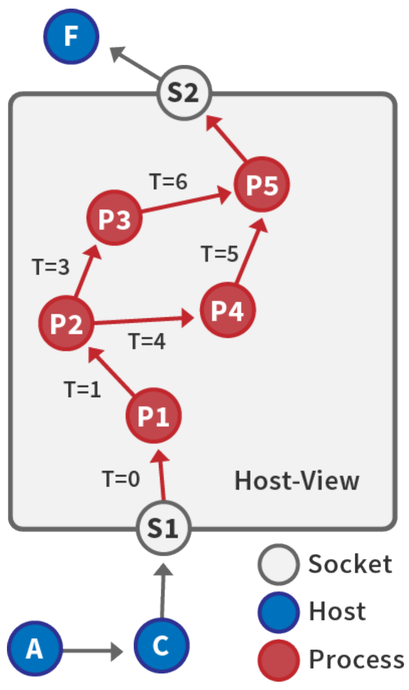
- We detect attacks by optimizing the deployment of our monitors
  - Our goal is to maximize our ability to detect attacks while minimizing the cost to do so
  - Monitors can also be compromised. We employ redundancy and statistical methods to detect compromised monitors
- Using our diverse monitors, we fuse different sources of data to increase the accuracy of our detection techniques, such as
  - Network level information
  - Host level information
  - Load and generator information

RESPONSE SELECTION ARCHITECTURE



- We leverage the outcomes of our fusion algorithms to drive our strategic response algorithms and commands to respond to different types of observed attacks
- Our goal is to build self-healing and self-reconfiguring networks to isolate infections and maintain operation.

SOME RESULTS FROM OUR WORK



- We built a detection scheme for Lateral Movement by fusing:
  - host-level process communication and,
  - network flow information
- We use process communication to infer correlation between network flows
  - Host-level agents collect the communication events *and* build a process communication graph
- Hierarchical fusion of events results in a **chain of correlated connections** that describes lateral movement in the system
- Detecting and stopping correlated chains helps preventing attackers from reaching **critical assets**

IMPACT ON STATE OF GRID SECURITY

Impacts on Your System

- Protected with proactive response algorithms, your system would:
  - detect attacks, reducing the manual load of monitoring alerts by human operators
  - contain an intrusion and provide semi-automatic response actions
  - run the system, possibly in a degraded state, until recovery is possible.

Business Benefit

- Reduced outages and complex manual processes
- Increased Data security and Cyber resilience

COLLABORATION OPPORTUNITIES

Cooperation, support and guidance from industry partners in the following areas would benefit this research activity:

- Specifications concerning the security requirements of the industry
- Datasets to better understand the systems and evaluate monitoring and detection techniques
- Discussions about the requirements for responses to attacks through control commands

- Contact: nouredd2@Illinois.edu, abohara2@Illinois.ed

- Activity webpage: https://cred-c.org/researchactivity/proresponse

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY