Mislead Physical-Disruption Attacks by Preemptive Anti-Reconnaissance for Power Grids Cyber-Physical Infrastructures

Hui Lin
Center of Cyber-Physical Intelligence and Security (CYPHER)
Electrical, Computer, and Biomedical Engineering Department
University of Rhode Island

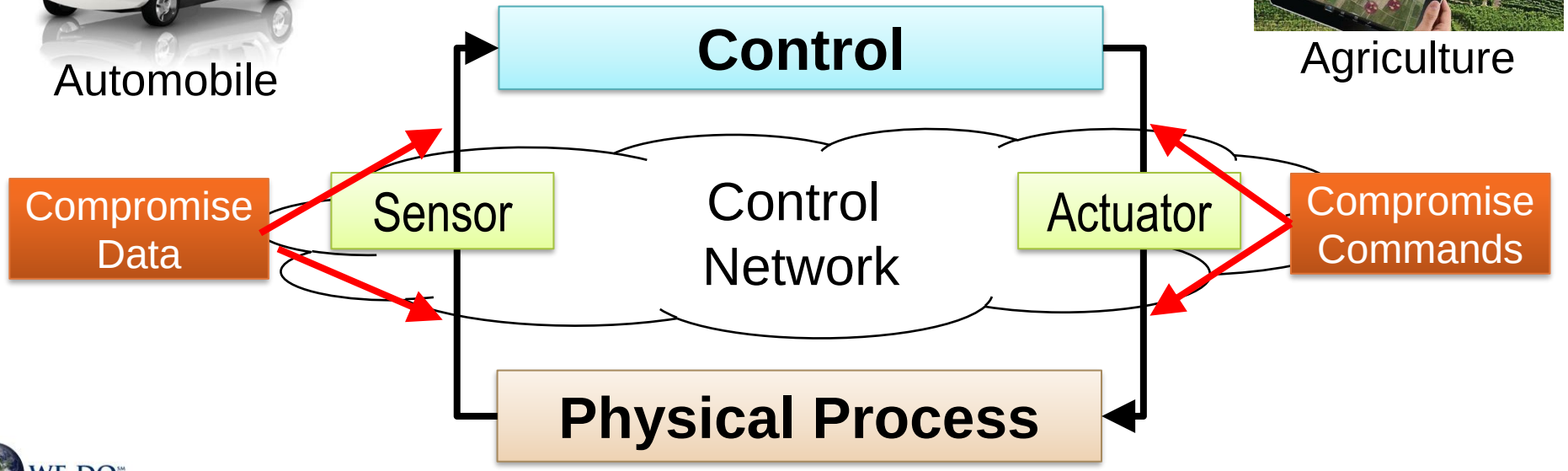
What are Cyber-Physical Systems

Medical Device

Power Grid

Agriculture

Automobile



THE DAILY SIGNAL

SEARCH

Ukraine Goes Dark: Russia-Attributed Hackers Take Down Power Grid

Riley Walters / January 13, 2016 / 1 comments

NATIONAL SECURITY

Stuxnet Raises 'Blowback' Risk In Cyberwar

WSJ.com - U.S. regulator says knocking out nine key substations could cause nationwide blackout

Energy sector tops list of US industries under cyber attack, says Homeland Security report

Researchers uncover holes that open power stations to hacking

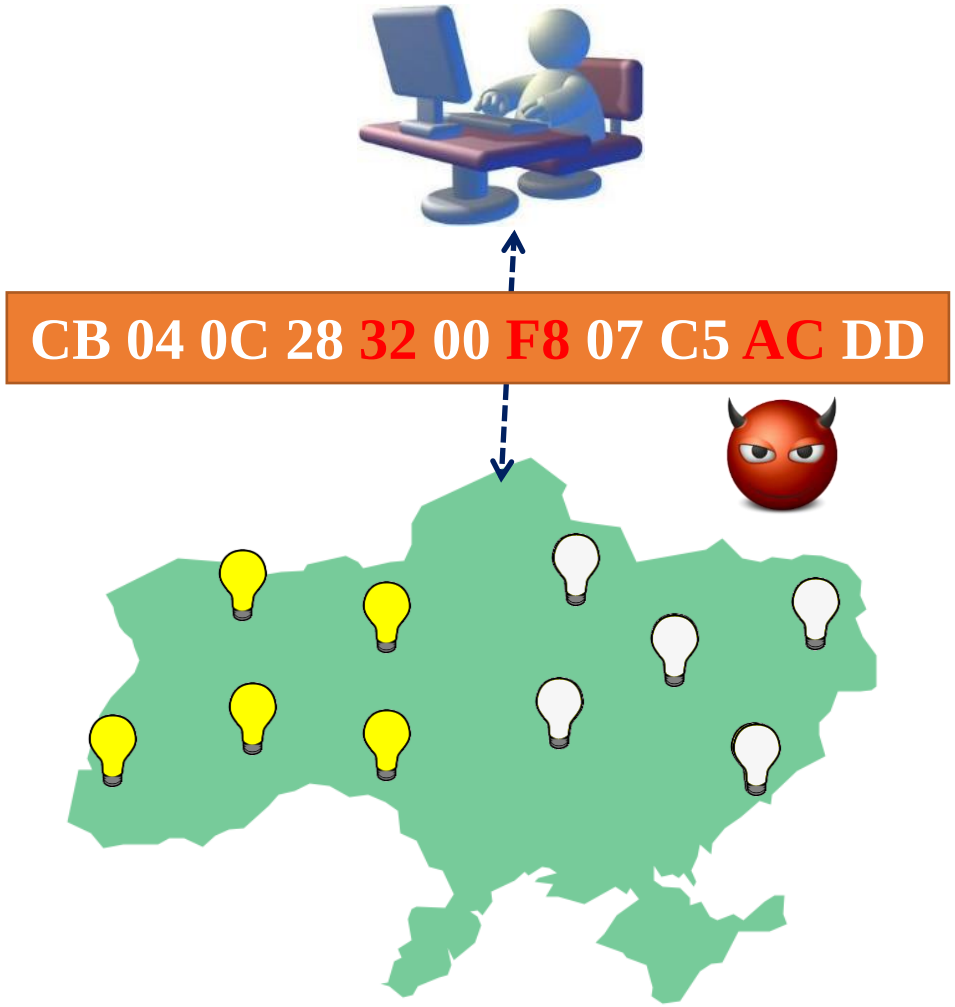
Hacks could cause power outages and don't need physical access to substations.

THE DAILY SIGNAL

SEARCH

Ukraine Goes Dark: Russia-Attributed Hackers Take Down Power Grid

Riley Walters / January 13, 2016 / 1 comments



"The attackers demonstrated a variety of capabilities, …, to gain a foothold into the Information Technology (IT) networks of the electricity companies."

"… the strongest capability of the attackers … in their capability to perform long-term reconnaissance operations required to learn the environment …"

"The outages were caused by the use of the control systems ..."
"… enabling the remote opening of breakers in a number of substations"

THINK BIG WE DO℠

CYPHER
Cyber-Physical Intelligence and Security

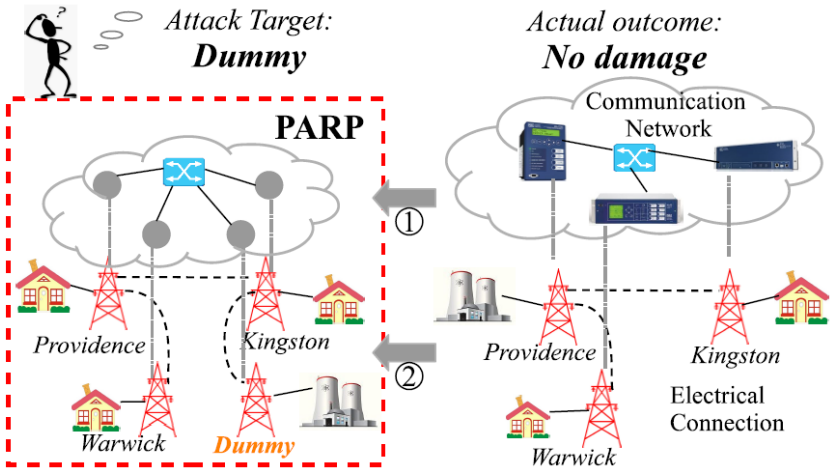
PARP: Mislead Physical-Disruption Attacks by Preemptive Anti-Reconnaissance for Power Grids' Cyber-Physical Infrastructures

Challenge:

- Adversaries perform in-depth reconnaissance, leading to irreversible damage
- How to mislead stealthy reconnaissance relying on legitimate operations
- How to craft misleading physical data

Solution:

- PARP, the first Preemptive Anti-Reconnaissance that will mislead adversaries about Power grids' cyber-physical infrastructures
- Technical approaches:
  - Control Function Virtualization (CFV), neutralizing communication pattern that can pinpoint physical device
  - Electrical-Model-Guided Adversarial Generative Networks (EleGAN), crafting decoy physical data conforming to power grids' physical models



Scientific Impact:

- Adversaries perform in-depth reconnaissance, leading to irreversible damage
- How to mislead stealthy reconnaissance relying on legitimate operations
- How to craft misleading physical data

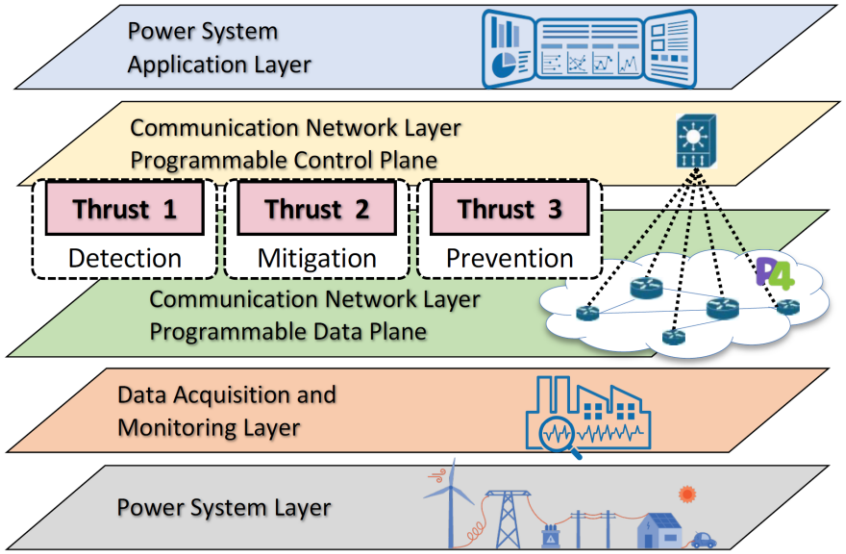
Enabling Programmable In-Network Security for an Attack-Resilient Smart Grid

Challenge:

- The underneath network infrastructure used by existing power grids significantly limits the performance of the existing security solutions

Solution:

- Create and quantify programmable in-network security measures for an attack-resilient power grid based on Programming Protocol-independent Packet Processors (P4) architecture
  - Customizing real-time in-network intrusion detection system in P4 programmable network switches
  - Creating network fault and vulnerability auto correction based on P4's traffic engineering hardware
  - Creating in-network traffic scheduler to disrupt attack reconnaissance by leveraging P4's hardware units



Scientific Impact:

- Advancing existing security solution with existing high-performance network devices
- Retrofitting power system application to programmable network infrastructure
- Creating next-generation high-performance security solution

CYPHER Mission

- URI CYPHER Center (Center of Cyber-Physical Intelligence and Security), established in summer 2020, is committed to advance fundamental research, technology advancement and transfer, as well as workforce and education development in broad domains of cyber-physical security and trustworthy artificial intelligence (AI).

- The Center currently has 12 faculty members, whose research addresses security challenges and AI advancement in power grid, computer networks, robotics, integrated circuits, high-performance computers and data centers.

Organization

Director: Yan (Lindsay) Sun, Computer Engineering, IEEE Fellow, NSF CAREER Awardee

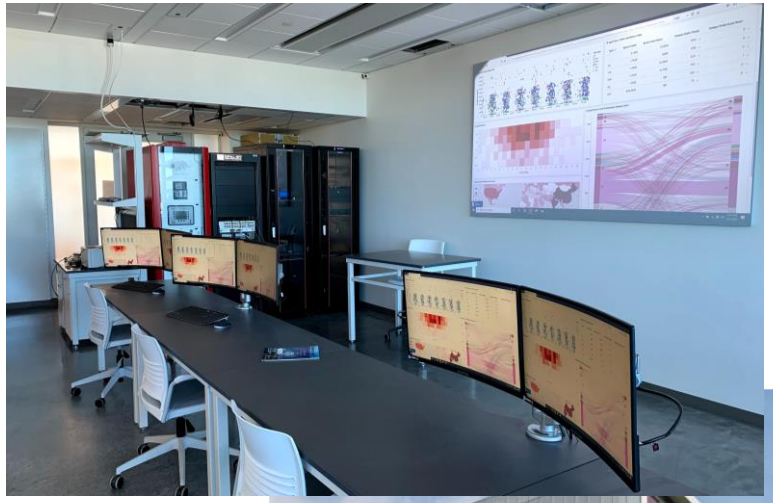
Co-Director: Haibo He, Electrical Engineering, IEEE Fellow, NSF CAREER Awardee

Technical Director: Tao Wei, Electrical Engineering, ONR YIP Awardee

Participating Faculty Members (alphabetically by last name)

- Kaushallya (Kay) Adhikari: Signal Processing, Information Theory
- Yeonho Jeong: Power Electronics
- Weiwei Jia: Operating Systems, Systems Virtualization, Modern Clouds
- Hui Lin: Cyber-Physical System, System/Network Security
- Resit Sendag: High-performance Computing, hardware acceleration;
- Manbir Sodhi: Optimization, Industrial Automation;
- Paolo Stegagno: Intelligence Robotics, Multi-agent Systems;
- Qing Yang: Computer Architecture; software-hardware co-design;
- Chengzhi Yuan: Adaptive Control, Robotics

Facilities



- CYPHER center, located in newly-established The Fascitelli Center for Advanced Engineering, has a lab space of more than 1,200 square feet, including advanced lab equipment:
  - OPAL-rt Real-Time Digital Simulator OP5700
  - Typhoon HIL602+ Ultra-High Fidelity Simulator
  - Intelligent Electronic Devices from Schweitzer Engineering Laboratories, Allen Bradley, and Schneider Electric
  - Programmable network devices and controllers