CPS and IoT Foundations: Performance and Resilience

Radha Poovendran
Professor and Chair
Department of Electrical Engineering
Director, Network Security Lab (NSL@UW)
University of Washington, Seattle
rp3@uw.edu

Outline

Resilience [DHS]:

(1) Ability to withstand disruption event with little loss in function

(2) Rapidly and efficiently restore functionality if loss incurred

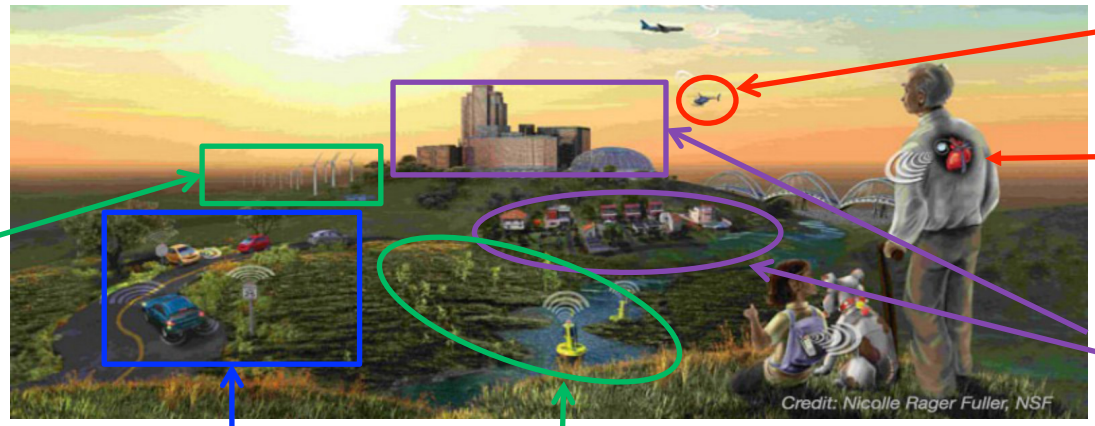
Three Topics in Resilience and Performance

Composition for Resilience and Performance

Resilience and Emerging Threats on Cyber-Physical Systems

Performance and Resilience with Human in the loop

Towards a Science of Composition for Performance and Resilience



Emergency Response

Health

Housing and Infrastructure

Energy

Transportation

Agriculture

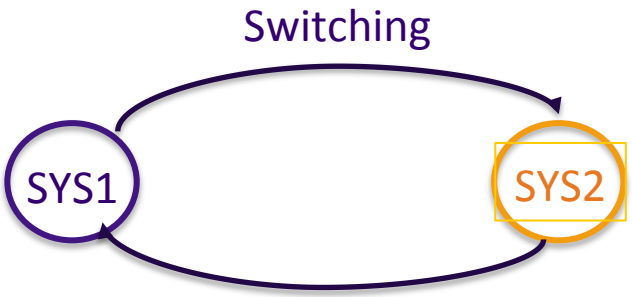
Large scale CPS is a system of systems with each subsystem being a CPS

Challenges:

- Ensuring performance and resilience of each component
- Guaranteeing **safety and availability** of the overall system

Need a **new design approach** for the science of composition

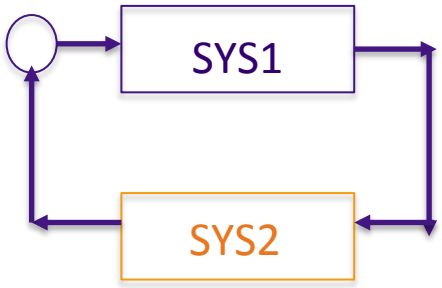
Challenges and Approaches for Composition for Performance and Resilience



First step: guarantee stability around desired operating point for each subsystem

Composition of stable systems **may not be stable** (Feedback interconnection, Switched systems…)

Possible approaches



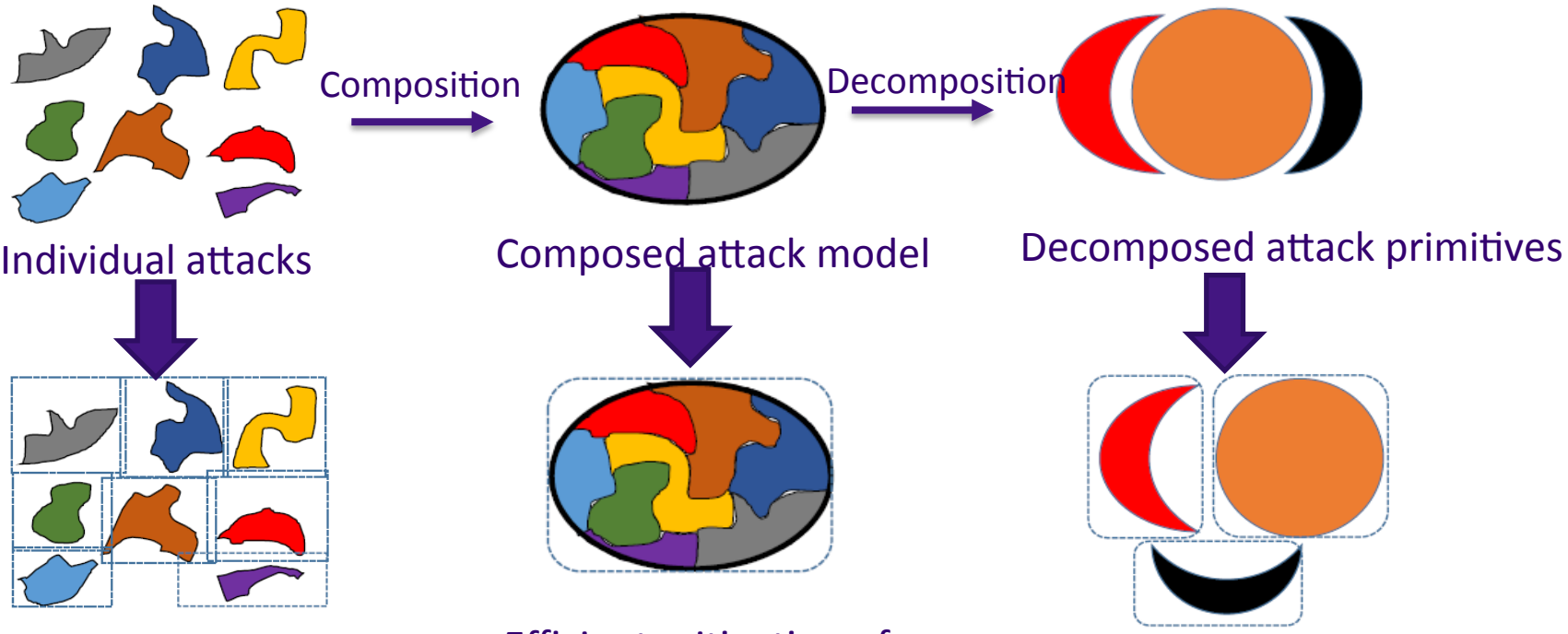
Composition of hybrid systems [Tabuada `09]

Passivity-based composition [Sztipanovits et al `12]

Each subsystem will be subject to multiple attacks

Can we provide compositional approach for security?

Passivity-Based Composition of Cyber Attacks

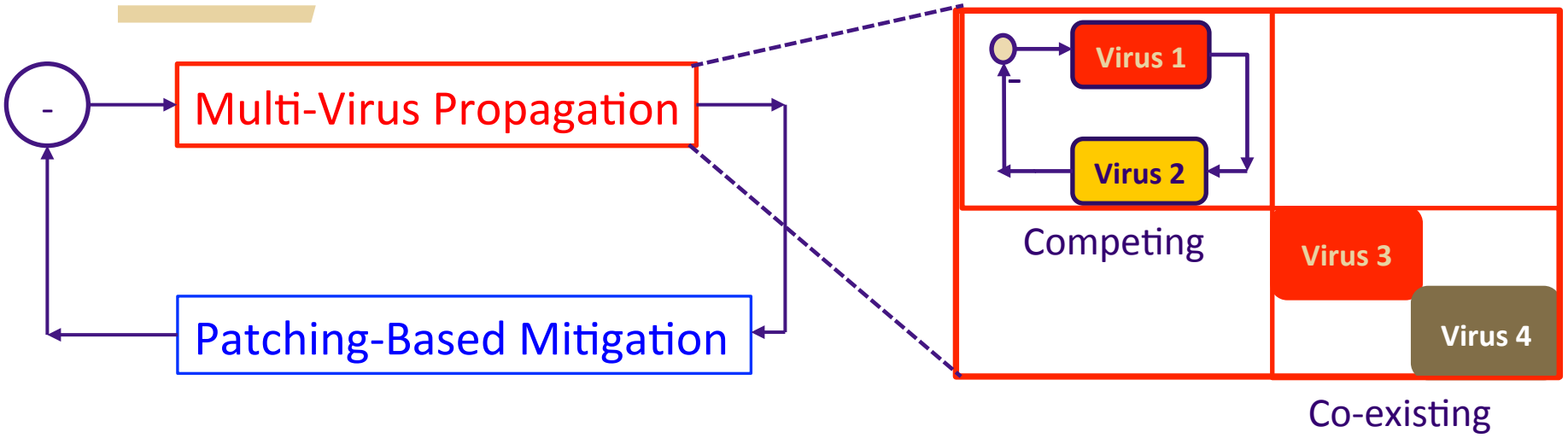


Questions:

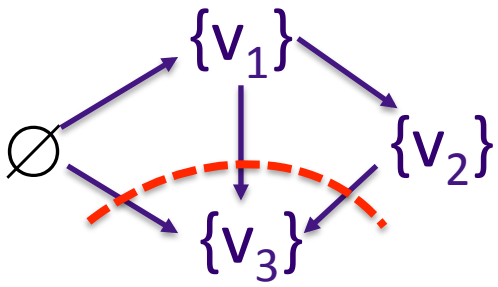
Identify class of attacks that admit passive representation

Quantify degree of deviation for attacks that do not admit passive representation

Passivity-Based Composition of Multi-Virus Propagation



The required patching rate is determined by the passivity index



Set of malwares: $\{v_1, v_2, v_3\}$

passivity index: maximum sum of transition rates into any v_i

Open Questions on Composition for Performance and Resilience

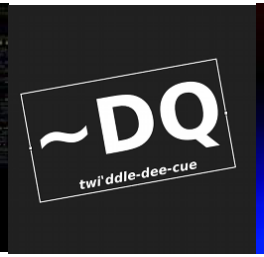
- Metrics to quantify uncertainty/deviation in developed model
- Compositions for joint performance and resilience
- Incorporate stochastic and adversarial uncertainties
- Ensure temporal and spatial scalability of composition
- Develop a science of decomposition for composed attack models
- Developing a decomposition approach for joint performance and resilience
- Integrate stochastic and dynamic interdependencies
- Design methods to disconnect subsystem for failure prevention (e.g., controlled islanding)
- Leverage interdependencies to prevent cascading failures

Emerging Threats on Cyber-Physical Systems: Advanced Persistent Threats (APTs)

- State-level actors with highly sophisticated attacks
- Cost of $375 – $575 billion annually
- Attacks targeting physical functionalities and data
- Stealthy and adaptive
- Persists for an extended period of time

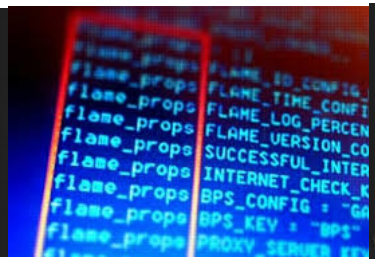
Stuxnet

2009



Duqu

2011

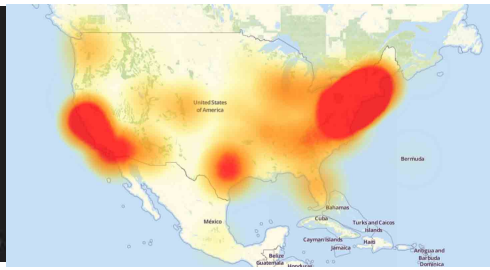


Flame

2012

Duqu 2.0

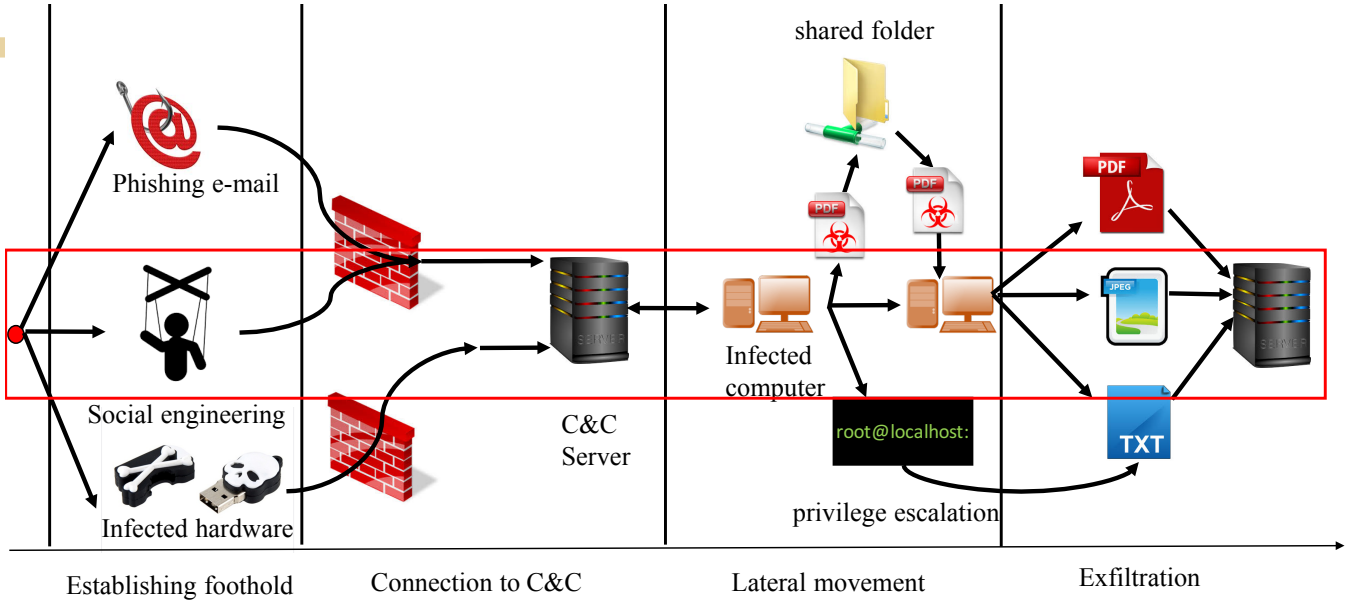
2015



October DoS attack

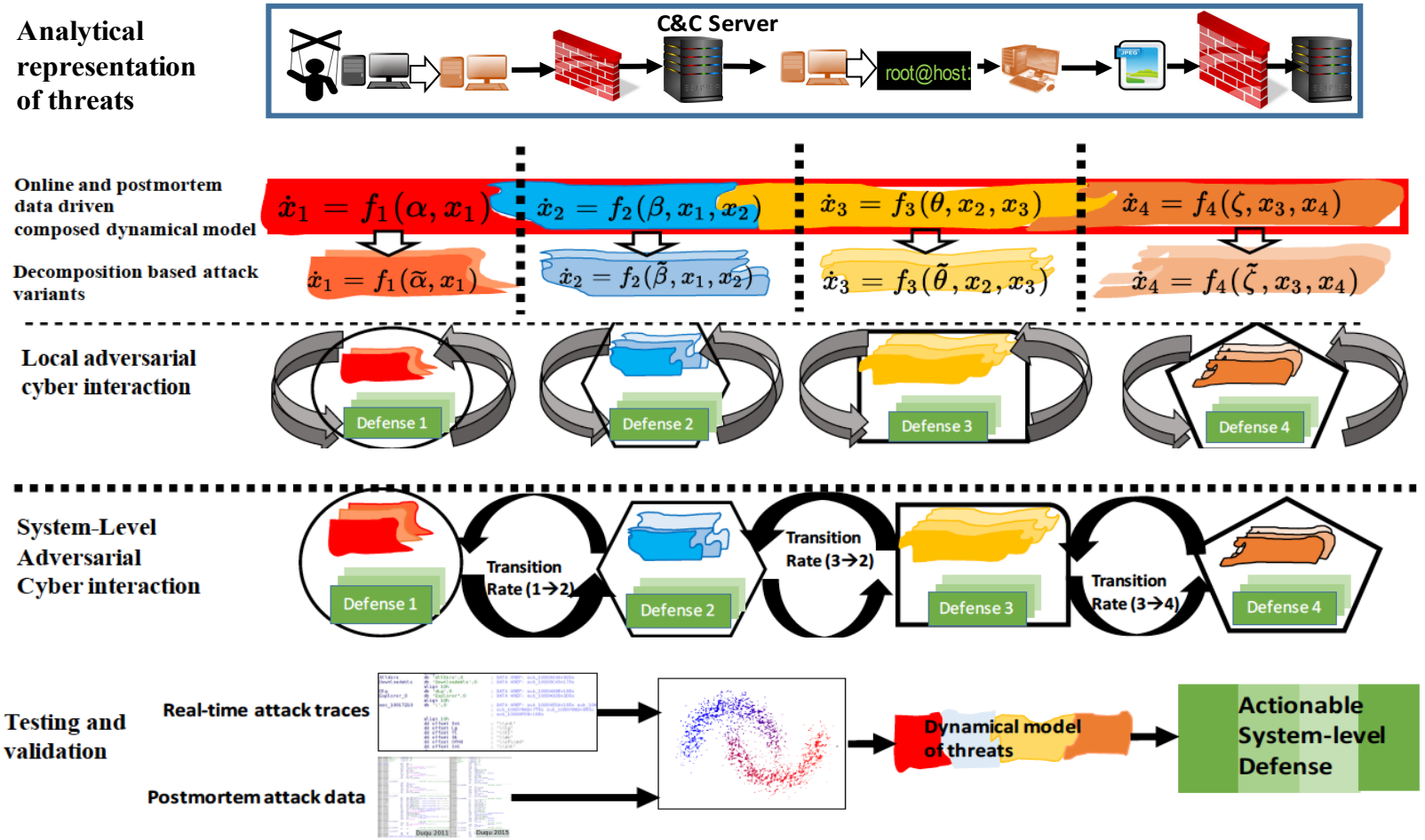
2016

Structure of Advanced Persistent Threats (APTs)

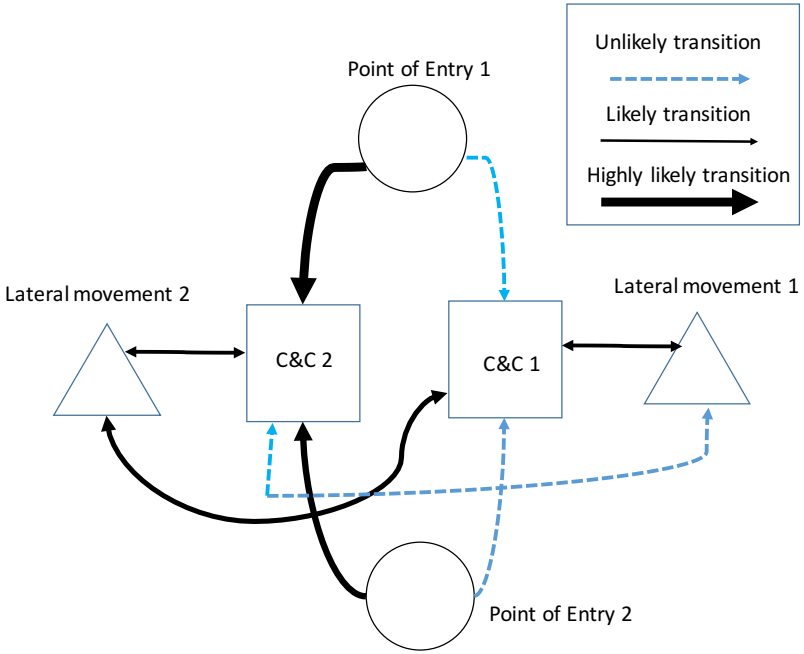


- Consists of **multiple attack stages**
  - Simultaneous attacks at different entry points
  - Sequential attacks that abruptly change
- Multiple **variants** that share identical steps
- **Persistent** and **adaptive**
- Exploits **zero-day** vulnerabilities

ADAPT: Analytical Framework for Actionable Defense against Advanced Persistent Threats



Learning under Deception



Goal: Refine the adversary model based on observed attack behavior

Challenges

- Adversarial learning in the presence of evasion and deception
- Quantification of uncertainty of adversarial representation

Open Questions: Emerging Threats on Cyber-Physical Systems

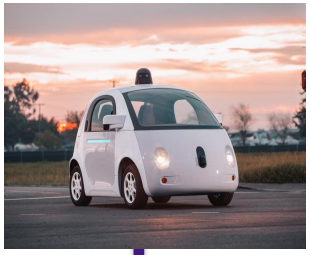
- Modeling interaction between system and adversary at each attack stage
- Identification of attack variants in each local stage
- Mitigation strategies for each local attack stage
- Make decisions with tampered data and deception
- Rules for composing different attack stages
- Can System-level defense strategies be obtained by composing local defenses?

Human in the Loop

Challenges:

- Tasks of CPS will be governed by human decision → Changes the performance requirement
- Requires a new level of guarantee for safety and resilience

Human in the Loop Modalities

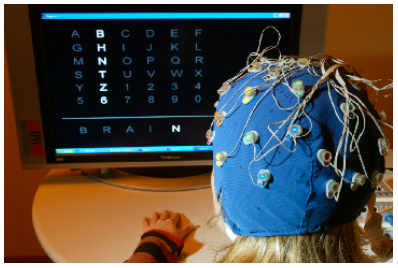


Human-operated

Semi-autonomous

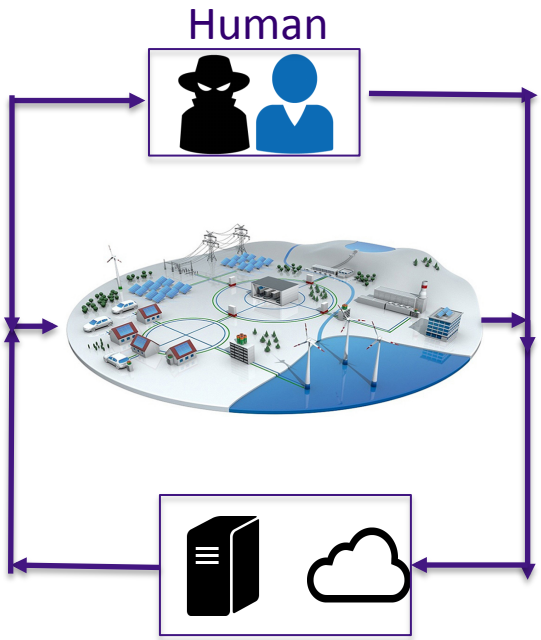
Fully-autonomous

Human machine interfaces



Level of autonomy and interface introduces new performance, security, and privacy requirements

Resilience of Human-Cyber-Physical System



Need to incorporate misbehaving and malicious human behaviors

Normal users can be compromised via social engineering

Challenge:
Provide services while penalizing misbehavior and avoiding malicious attacks

Possible approaches:
Game-theoretic incentive design [Sastry et al]

Open Questions: Providing Resilience with Human-in-the Loop

- Computational modeling human behavior (Bounded rationality, limited cognition, and time-delay)
- Detecting adversarial human behavior
- Optimal control-sharing between human and CPS
- Design usable CPS interfaces while satisfying resilience requirement
- Learning human behavior with safety and privacy constraints
- Developing verification methods of correct human behavior

Broader Questions

- Can we derive Science Laws for joint performance and resilience in CPS domains?
- Bounds on the impact of an attack on the performance and resilience
- Learn, compute, and estimate in the presence of deception
- Factoring Computational Social Component into performance and resilience across CPS domains