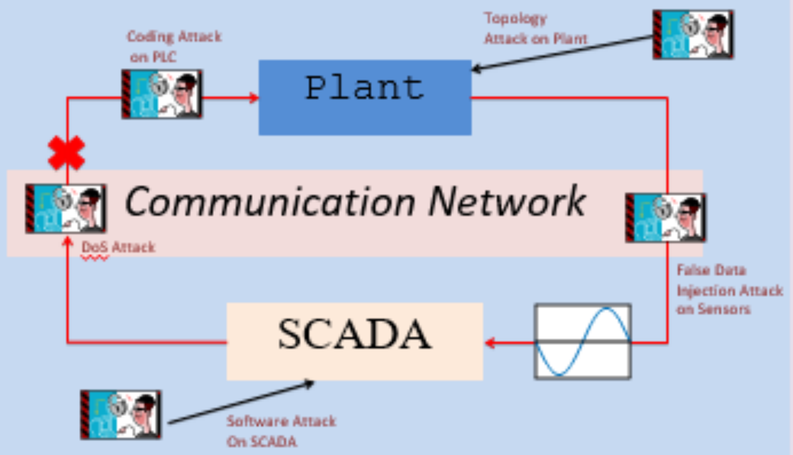
CPS Synergy: Information Flow Analysis for Cyber-Physical System Security

PI Bruno Sinopoli (Washington University in St Louis), Co-PI Soummya Kar, Co-PI Anupam Datta (Carnegie Mellon)

Challenge

The Resiliency of CPS Must Be Addressed

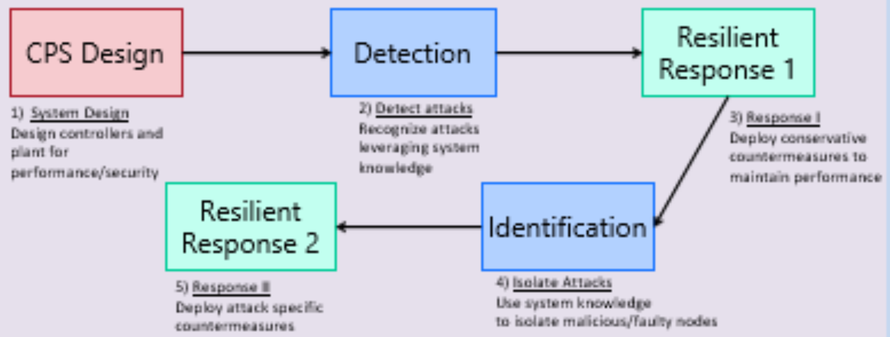


We Lack a Unifying Framework

Cyber + Software Security + System Theory

A Framework of Accountability

Encompasses Detection, Identification, Correction



Information Flow Anaysis: A Language for CPS Security

An information flow exists from *x* to *y* when information in *x* is transferred to, or used to or derive information transferred to *y*

Traditionally used to restrict flows for secrecy/privacy

Example: US Intelligence: Unclassified ≤ Confidential ≤ Secret ≤ Top Secret → **Valid Information Flow**

Noninterference: the absence of information flow can be used to express diverse security policies

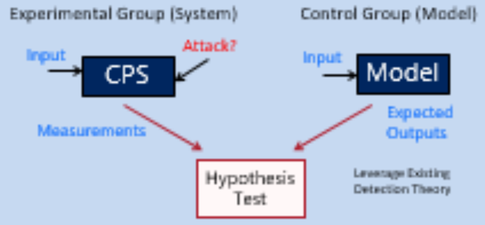
Multi Level Security | Discretionary Access Control | Capability Passing | Confinement

Information Flow for Detection

Detecting Flows of Information: ***Example Web Data Usage Detection***

Does browser history affect the Ads one receives?

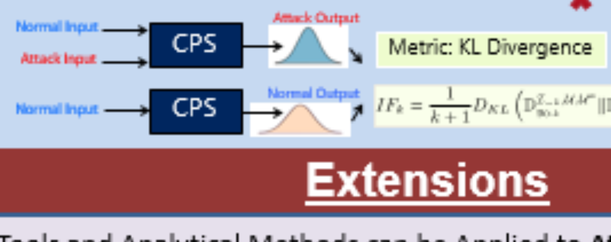
Answer Via Information Flow Experiment



In CPS Security we wish to detect an information flow from the attacker's inputs to the defender's outputs.

Desire a Causal Measure of Information Flow: The KL Divergence

Causal Measures: Quantify cause and effect. Useful for detection.



Quantify the effect of the attacker's inputs on system outputs

$$IF_k = \frac{1}{k+1} D_{KL}\left(\mathbb{D}^{\bar{Y}_{0:k}|\mathcal{M},\mathcal{M}^a} \,\|\, \mathbb{D}^{\bar{Y}_{0:k}|\mathcal{M},\mathcal{M}^0}\right)$$

Relates to fundamental limits on attack detectability

Design Methodology

Goal: Be able to detect new attack vector by designing IF > ε

1) Attacker Policy | Current Defender Policy | Defender Degrees of Freedom → Categorize Information Flow

2) Do the Following

Type of Information Flow	Detectability of Attack	Action Required
Unconditional ε - weak information flow	Attack is stealthy for all admissible defender policies: IF ≤ ε	Nothing can be done without increasing the available DOF for the defender
Conditional ε - weak information flow	Attack is stealthy for some defender policies (including current): IF ≤ ε	Change Policy: Balance Information Flow and System Performance
ε – strong information flow	Attack is detectable for current defender policy: IF > ε	None

Large Information Flow ⟷ Attack is Detectable

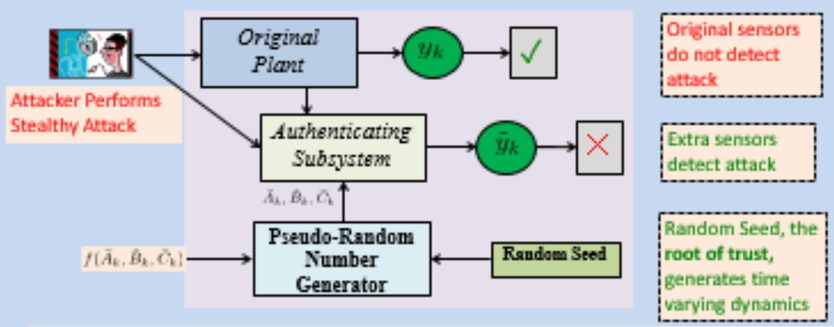
3) If necessary, increase degrees of freedom and/or change the defender policy. Ensure prior attack vectors generate sufficient Information Flow

Example: Moving Target Defense

Attack strategy *Ua* generates **unconditional ε – weak information flow**

Illustrated Examples: Zero Dynamics, False Data Injection Attacks

Action: increase DOF by introducing authenticating subsystem



Even if a system is susceptible to strong attackers such as malicious insiders or nation state adversaries, the moving target defense elicits an **ε – strong information flow**

Extensions

Tools and Analytical Methods can be Applied to **Attack Identification**

Design Measures | Node *i* attacked → Large IF(i) | Node *i* normal → Small IF(i)

Use Traitor Tracing research to develop efficient algorithms

Information Flow Analysis can help us bridge the gap between mainstream security + privacy and system theory

Ex 1: Compositional Security

Ex 2: Apply privacy related information flow techniques to system theory

Impact: By integrating information flow, a traditional cyber security centric notion, and resilient control of physical systems, this project will enable unified foundations of CPS security for researchers.

Affects: traditional CPS such as the Smart Grid and Transportation Systems as well as emerging fields such as network science and the Internet-of-Things (IoT). Benefits operators, researchers, society at large.

Education and Outreach: A course of CPS security/Information flow, Aid to Minority Serving Institutions, SEE Program for High School Students

2019 NSF Cyber-Physical Systems Principal Investigators' Meeting
November 21-22, 2019 | Crystal City, Virginia

Award ID#: 1646526