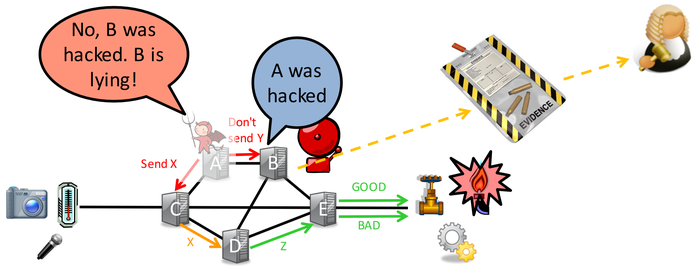
Synergy: Collaborative Research: Security and Privacy-Aware Cyber-Physical Systems

PI: Insup Lee, University of Pennsylvania (lee@cis.upenn.edu)

2015 CPS PI MEETING

Task 1: Platform support for security



Scenario: Compromised control node

- Attacker has full control over one node; tries to cause damage

What should the system do in this case?

- ***Detection***: Quickly alert an operator
- ***Recovery***: Stop, if possible, continue running
- ***Forensics***: Tell us what happened
- ***Evidence***: Prove responsibility / liability

Challenge: Attacker may try to prevent these.

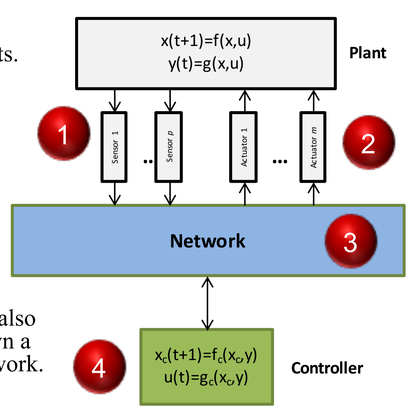
Task 2: Security-Aware Control Design Attacks on Control Systems

1. Sensor attacks
The attacker can arbitrarily change sensor measurements.

2. Actuator attacks
The attacker can arbitrarily change actuator values.

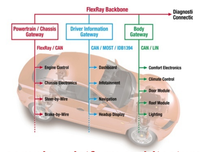
3. Communication attacks
The attacker can change messages between sensors-controllers or controllers-actuators. The attacker can also inject messages to shut down a controller or the whole network.

4. Controller attacks
The attacker can change the controllers' parameters, resources (e.g., execution model) or even the controllers' code.

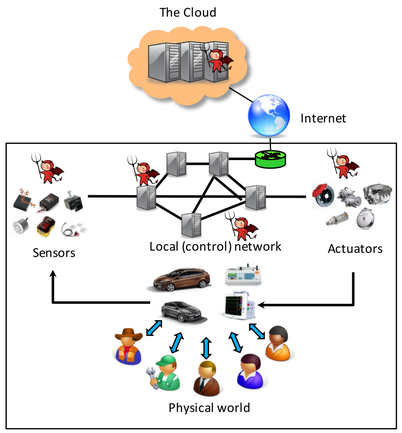


Project Overview

***Goals of the project*: to develop a framework in which the mix of prevention, detection, recovery and robust techniques work together to improve the security and privacy of CPS.**

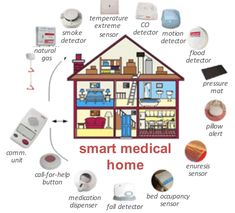


complex platform architecture

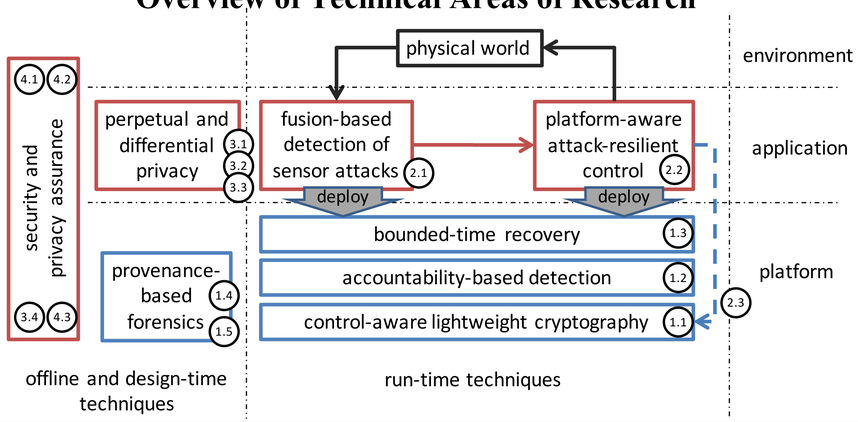


Internet-connected car

medical devices



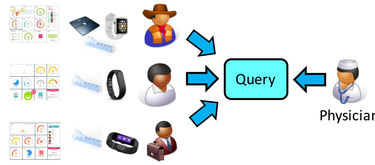
Overview of Technical Areas of Research



Team

Insup Lee (PI, Penn)
Andreas Haeberlen (Penn)
Bill Hanson (UPHS)
Nadia Heninger (Penn)
Ross Koppel (Penn)
Miroslav Pajic (Duke)
George Pappas (Penn)
Linh Phan (Penn)
Rita Powell (Penn)
Kang G. Shin (Michigan)
Oleg Sokolsky (Penn)
Jeffrey Vagle (Penn)
Christopher Yoo (Penn)
Jesse Walker (Intel)

Task 3: Working with Sensitive Data



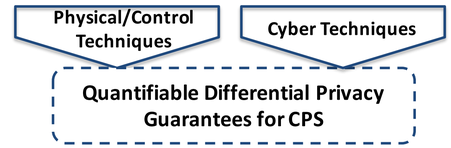
Who	What
Bob	Drug A
Charlie	Drug B
Fannie	Drug B
George	Drug A

Example: "Does drug XYZ work better during rest periods, or during heavy exercise?"

***Problem*:**

Differential privacy guarantees for distributed systems while processing continuous data streams.

***Our approach*:**



Task 4: Modeling Human Factors

***Problem*:**

Users resort to workarounds when they feel that security features of a system prevent them from doing their work. How can we predict workarounds and analyze their effects?

***Proposed approach*:**

- Model potential workarounds as hazards and apply risk analysis
- Incorporate users' mental models into model-based design of CPS

Collaboration Structure