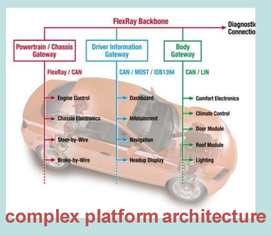
Security and Privacy-Aware Cyber-Physical Systems

Lead PI: Insup Lee (U. Penn), PIs: Miroslav Pajic (Duke U.), Kang G Shin (U. Michigan)

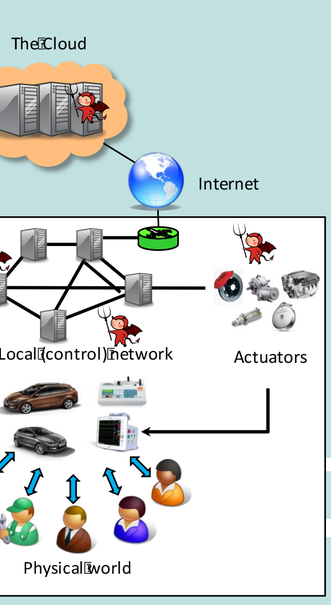
https://rtg.cis.upenn.edu/cps-security

The objective of this project is 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

Ubiquitous interconnected devices enable new capabilities but create new security and privacy risks

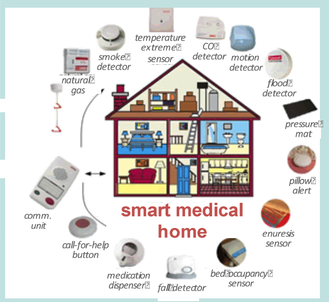


complex platform architecture

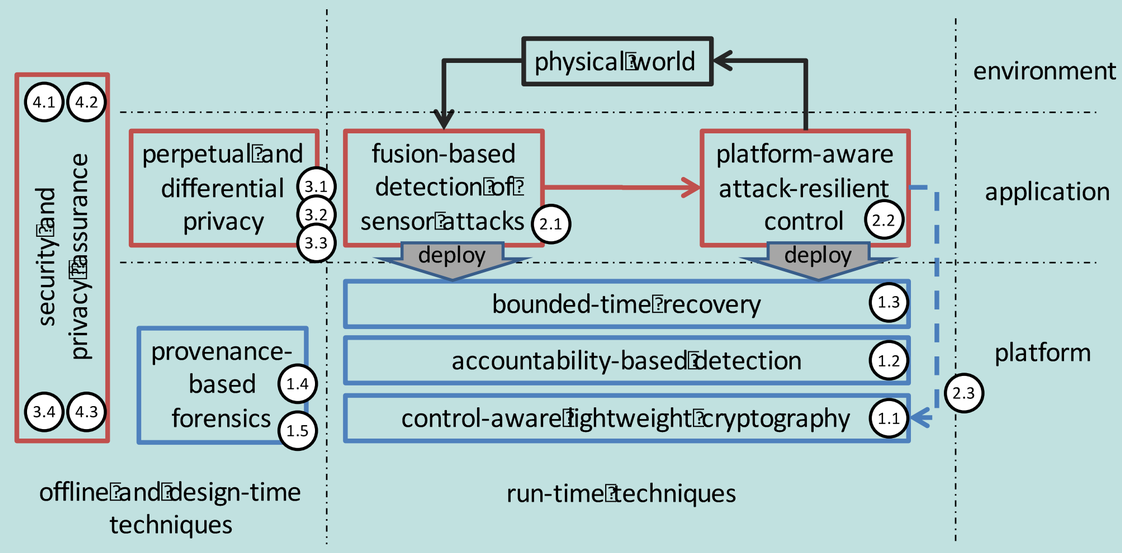


Internet-connected car

medical devices



Overview of the Technical Approach

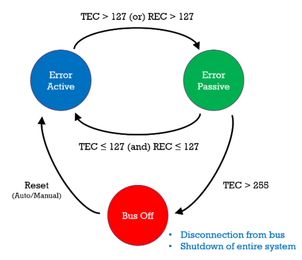


Platform support for security

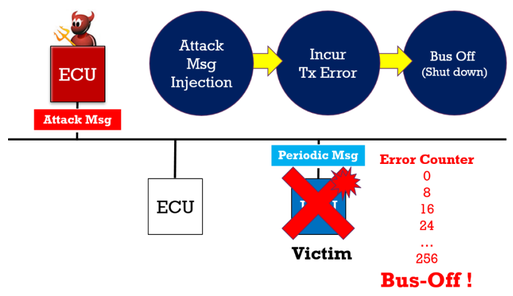
Attack Model: "Bus-off Attack"

-Attacker's objective is to shut down or disconnect uncompromised (healthy) in-vehicle ECUs with minimal number of injections.

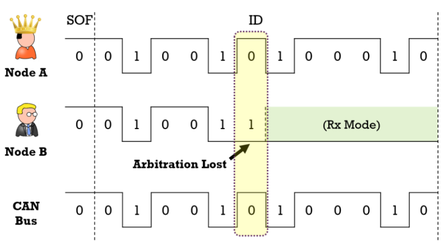
- Exploit the error handling mechanism in CAN and deceive the victim into thinking it is erroneous while is actually under attack.



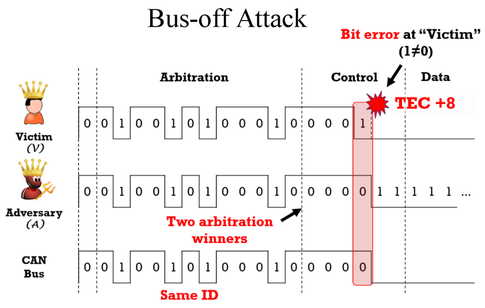
CAN Error Handling Mechanism



Bus-off Attack



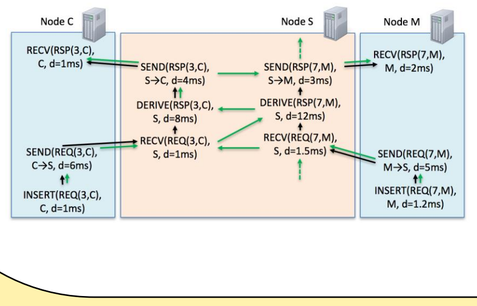
Only ONE arbitration winner !

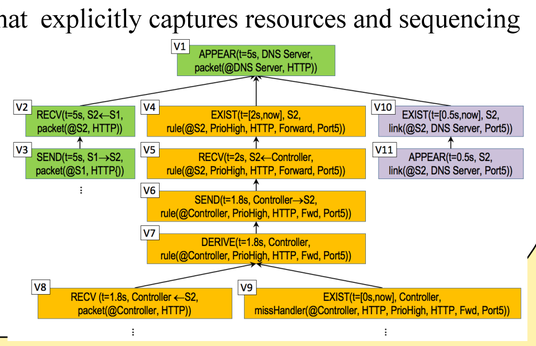


But in the bus-off attack... TWO arbitration winners

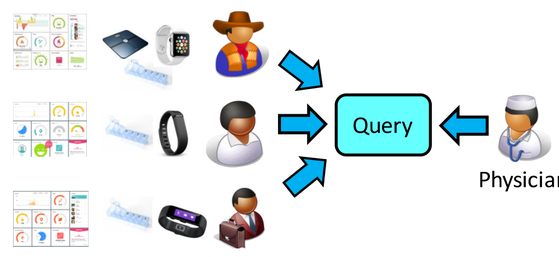
How do we figure out what happened?

- Goal: System should be able to 'explain' to a forensic investigator why a given event occurred
- Idea: adapt the concept of data provenance from the database literature
- Problem: existing solutions only explain functional behavior ("why did this happen?") but not temporal behavior ("why did it happen too late?", "why did it take so long?")
- Approach: new time-aware provenance model that explicitly captures resources and sequencing





Working with Sensitive Data



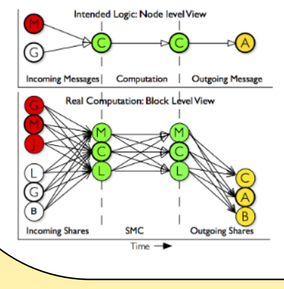
Who	What
Bob	Drug A
Charlie	Drug B
Fannie	Drug B
George	Drug A

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

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

Approaches

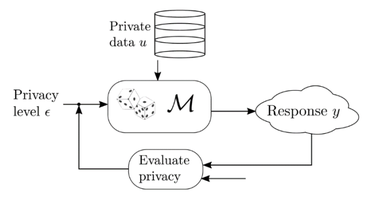
Distributed queries for differential privacy



- data never leaves user domain

Run-time differential privacy

A privacy-preserving mechanism that allows online relaxing privacy.



Security-Aware Control Design

Attack-Resilient State Estimation for Noisy Dynamical Systems

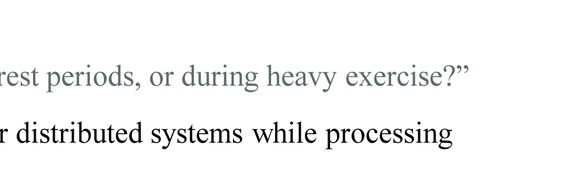
$$P_{0,\omega}: \min_{\tilde{\mathbf{e}},\mathbf{x}} \|\tilde{\mathbf{e}}\|_{l_2,l_0} \qquad P_{1,\omega}: \min_{\tilde{\mathbf{e}},\mathbf{x}} \|\tilde{\mathbf{e}}\|_{l_2,l_1}$$

$$s.t. \quad \tilde{\mathbf{y}} - \mathbf{O}\,\mathbf{x}_0 - \tilde{\mathbf{e}} = \tilde{\mathbf{w}}, \quad \tilde{\mathbf{w}} \in \Omega$$

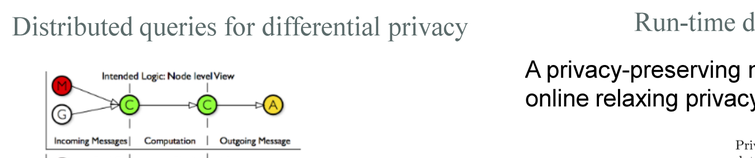
Formal robustness guarantees for the optimal l_0 and convex l_1 estimator

Relaxing Integrity Requirements for CPS

Sporadic integrity enforcement: If at step k, sensor integrity is enforced (e.g., with the use of MAC), then $\mathbf{a}\downarrow k = 0$.

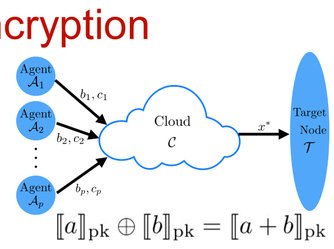


Theorem [Jovanov&Pajic'16]: Even with sporadic sensor integrity enforcement, the attacker cannot introduce unbounded estimation error.



Limiting attack effects: Trajectory following study – attack induced estimation error < 5 cm when <20% of CAN packets contain MAC

Optimization and Control using Partially Homomorphic Encryption



$$[\![a]\!]_{\mathrm{pk}} \oplus [\![b]\!]_{\mathrm{pk}} = [\![a+b]\!]_{\mathrm{pk}}$$

Privacy-aware cloud-based optimization over sensitive data:

- Agents encrypt information before sending to untrusted cloud
- Cloud computes optimal solution without learning the sensitive data or the final solution

Interested in meeting the PIs? Attach post-it note below!

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

National Science Foundation WHERE DISCOVERIES BEGIN

intel

Penn Engineering

University of Michigan

Duke University