Security vs. Privacy in Cyber-Physical Systems

Luis Burbano[1], Gabriel Torres[1], Mestan Celiktug[2], Alvaro Cardenas[1], Murat Kantarcioglu[2] and Jonathan Katz[3].

[1]Univertisy of California at Santa Cruz, [2]University of Texas at Dallas, [3]University of Maryland

Abstract: This research examines the scientific foundations for modeling security and privacy trade-offs in cyber-physical systems, focusing in particular on settings where privacy-protection technologies might be abused by malicious parties to hide their attacks. The goal is to provide both security and privacy guarantees for a variety of cyber-physical systems.

Challenges

- Preserve confidentiality and security of outsourced control computation and attack detection to the cloud for cyber-physical systems.
- Overhead of confidentiality preserving techniques for a real-time control system.
- Tradeoffs between varying levels of confidentiality. Some methods require some parameters to be public (homomorphic encryption). Methods that ensure all parameters are confidential may be too expensive in practice (fully homomorphic encryption), while others might require a high amount of network communication (garbled circuits).
- Anomaly detection computations may require computations that are more complicated on encrypted data.

Assumptions

- We assume the system matrices are public while the sensor measurements $\boldsymbol{y}$, state estimation from the estimator $\hat{\boldsymbol{x}}$, control signal $\boldsymbol{u}[k]$, references $\boldsymbol{u}_r, \boldsymbol{x}_r$, and anomaly detection parameters are kept private.
- Clouds are honest-but-curious. That is, clouds honestly follow the algorithms, but they want to learn information about the system.

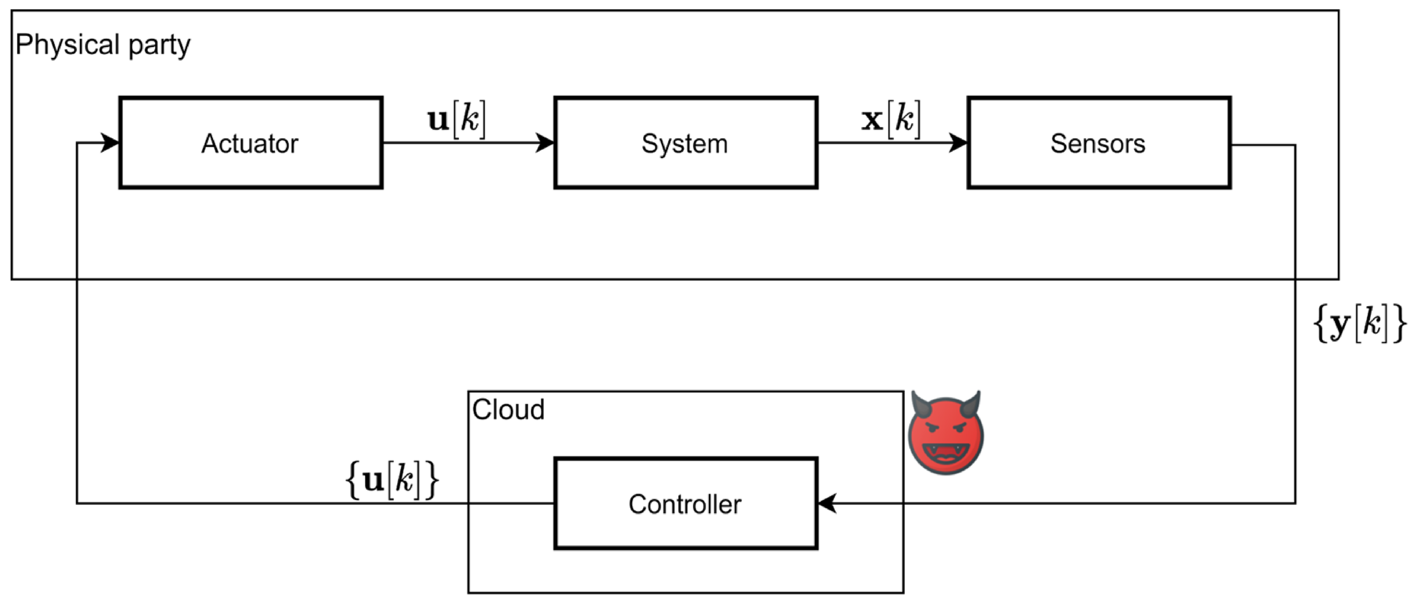
Solutions

- Implement different solutions not commonly used in control systems to maintain confidentiality such as,
  - Homomorphic Encryption.
  - Garbled Circuits.
- Develop model-based anomaly detection to detect attacks on sensor measurements for linear-time invariant systems in a privacy setting.
- Employ trusted execution environments (TEEs) to maintain security and confidentiality of control computations.

Methods

We are going to implement the control while maintaining sensible information private in a linear time-invariant system. We will use an LQG controller in the cyber world to compute the control action, $\boldsymbol{u}[k]$, from an encrypted sensor signal, $\{\boldsymbol{y}[k]\}$, from the physical world.

We will also implement anomaly detection in the cloud. A state estimator will be used to predict the system state and compute the distance between the current and expected measurements called the residues. To identify an anomaly, we are going to use the nonparametric cumulative sum (CUSUM), which uses the residue to compute a statistic, $s[k]$. An alarm is triggered when $s[k] > \tau$ where τ is a threshold.



Impact

- Demonstrate the feasibility of maintaining confidentiality, using multi-party computation and encryption techniques in processes that require continuous communication of sensor measurements and control commands.
- Industrial cyber-physical systems are protected from attacks while outsourcing computations to a third-party; an attacker would require more effort to deploy dangerous attacks.
- Users of cyber-physical systems could keep their sensitive information private. For example, in autonomous vehicle platooning (vehicles cooperate to maintain a desired distance between them), vehicles want to keep information (e.g., position, velocity) private.

[1] A. B. Alexandru and G. J. Pappas, "Encrypted LQG using labeled homomorphic encryption," in Proceedings of the 10th ACM/IEEE international conference on cyber-physical systems, 2019, pp. 129–140.

UC SANTA CRUZ

Baskin Engineering UC SANTA CRUZ