# First Workshop on Cyber-Physical Systems Security and PrivaCy (CPS-SPC): Challenges and Research Directions

Roshan K. Thomas
The MITRE Corporation

Alvaro A. Cárdenas
University of Texas at Dallas

Rakesh B. Bobba
Oregon State University

## ABSTRACT

The First International Workshop on Cyber-Physical Systems Security and PrivaCy (CPS-SPC) is being held in conjunction with the 22nd ACM CCS Conference. The workshop was motivated by several observations. First, cyber-physical systems represent the new frontier for cyber risk. The attack surface imposed by the convergence of computing, communications and physical control represents unique challenges for security researchers and practitioners. Second, most published literature addressing the security and privacy of CPS reflect a field still in its infancy. As such, the overall principles, models, and theories for securing CPS have not yet emerged. Third, the organizers of this workshop strongly felt that a premiere forum associated with a premiere conference was needed for rapidly publishing diverse, multidisciplinary in-progress work on the security and privacy of CPS and galvanizing the research community. The set of accepted papers reflect this vision. Papers span cyber and control-theoretic foundations, intrusion detection, forensics management, vulnerability analysis and elimination, and field studies. We have organized an exciting program for this workshop and look forward to active participation in this and future workshops.

## Categories and Subject Descriptors

H.4 [**Information Systems Applications**]: Miscellaneous

## Keywords

CPS Security and Privacy

## 1. INTRODUCTION

Cyber-physical systems (CPS) integrate computing and communication capabilities with monitoring and control of entities in the physical world. These systems are usually composed by a set of networked agents, including sensors, actuators, control processing units, and communication devices. While some forms of CPS are already in use, the widespread growth of wireless embedded sensors and actuators is creating several new applications in areas such as medical devices, automotive, and smart infrastructure. Equally important is the emergence of Internet of Things (IoT) and how IoT will interface with control systems. As such, there is an increasing role that cyber infrastructures will play in existing control systems and in domains as diverse as the process control industry, the power grid, transportation systems, and medical devices and systems.

Many CPS applications are safety-critical: their failure can cause irreparable harm to the physical system under control and to the people who depend on it. In particular, the protection of our critical infrastructures that rely on CPS, such as the electric power transmission and distribution, industrial control systems, oil and natural gas systems, water and waste-water treatment plants, healthcare devices, and transportation networks play a fundamental and large-scale role in our society—and their disruption can have a significant impact to individuals, and nations at large.

Similarly, because many CPS systems collect sensor data non-intrusively, users of these systems are often unaware of their exposure. Therefore in addition to security, CPS systems must be designed with privacy considerations.

The challenges in securing CPS are many. But fundamentally, it is important to recognize that securing CPS differs from the traditional cyber security concerns of confidentiality, integrity and availability (CIA) that have dominated the security of information technology (IT) systems. At its core, CPS security must be approached and framed from the perspective of how attacks on CIA properties perturb control-theoretic properties such as controllability, observability and stability.

## 2. OBJECTIVE AND SCOPE

The objective and vision of the workshop is that it becomes the premiere forum to publish research on CPS security and privacy. As such this first workshop sought to set this vision on solid footing, and invited participation from diverse CPS domains, researchers and practitioners, and encompassed a range of topics. Submissions were sought from multiple interdisciplinary backgrounds representative of CPS, including but not limited to information security, control theory, embedded systems, and human factors.

To help establish a solid footing for the workshop, we have documented below some major research challenges and promising directions. We hope that the CPS-SPC community will build upon and add to this list of challenges and research directions over the years.


*CCS'15,* October 12–16, 2015, Denver, Colorado, USA.
ACM 978-1-4503-3832-5/15/10.
DOI: http://dx.doi.org/10.1145/2810103.2812621 .

### *Trust Modeling and Human-in-the-Loop.*

The issue of modeling and managing trust between the control system and the operator, as well as between components of the control system, remains one of the most prominent and emerging challenges. As far as trust between the control system and the operator, consider the crash on May 31st, 2009 of Air France Flight 447 enroute from Rio de Janeiro, Brazil to Paris, France. Temporary inconsistencies in both airspeed sensors resulted in the flight control system disengaging autopilot and autothrottle. In other words, the control system was designed to give control back to the pilot (operator) when sensing anomalies occurred, based on the principle that the pilot is more knowledgeable and can be trusted to handle the situation better. Unfortunately, in this case the pilot made an abrupt nose-up input which resulted in an intolerable angle of attack and the aircraft stalling and crashing. Perhaps a better design may have been one where the control system used additional sensors to possibly extrapolate the air speed. For example, the engine speed and the altitude could be correlated to make reasonable guess that the aircraft could not be traveling at 52 knots (as indicated by the faulty sensors). Trust management between the components of a control system is also a challenging area for future work. In particular, a cyber-attack could subvert a component whereby the compromised component now becomes a malicious insider. System designs which recognize the criticality and trustworthiness of control system components are required. This obviously requires schemes for continuously assessing and managing such trustworthiness.

### *Cognition, Situational Awareness and Security.*

Increasingly many CPS are operated under automated controls. In such operations, the operator has a secondary or in many cases a minimal role in routine operations. The problem is exacerbated when operator fatigue sets in. A sophisticated cyber-attack can exploit such weaknesses to its advantage. Specific attack steps can be crafted knowing that operator SA will be low at specific times. Mitigating this will require system man-machine interface designs that continually sense operator fatigue and cognitive load. Alert mechanisms have to be multimodal (not just on operator screens). Also, the control system functions and communications that generate them must be designed in a manner that they cannot be bypassed by cyber attacks.

### *High Assurance Architecture Challenges.*

Size, weight and power (SWAP) considerations are driving the evolution of system architectures for CPS. For example, in the avionics industry, early designs of avionics systems used a federated architecture where every function had its own dedicated line replaceable unit (LRU) computer and was connected to its own sensors and actuators. However, as more control functions get automated through digital controls, the weight, volume, and maintenance overhead of each system made this approach not sustainable. A new approach, called IMA (Integrated Modular Avionics), integrated multiple software functions on a single processor so as to keep the weight, volume and cost of the avionic architecture within reasonable limits. Strict partitioning in software and hardware had to be provided to ensure that functions did not interfere with each other. These developments are found in the ARINC 653 and ARINC 664 standards. ARINC 653 recognizes different safety levels for applications. Additional research is needed to bring separation kernels and associated information flow controls, data isolation, fault isolation, and schedule-related QoS guarantees in these emerging architectures for control system processors.

### *Security vs. Safety.*

Traditionally, CPS designs have always accounted for safety. Safety analyses such as with fault trees typically assume that faults are random and benign. Many CPS are designed to mitigate at most one fault at any given time. Such assumptions no longer hold in the face of sophisticated and malicious cyber attacks. Such an attack may launch concurrent actions that induce multiple simultaneous faults in a coordinated manner. While safety designs typically incorporate checks and balances and related compensating actions, these could be intercepted by a cyber attack. Furthermore, while safety concerns encourage a fail-open principle of operation, security concerns often demand a fail-close approach. As such, an important research challenge is to understand and formalize the interplay between security and safety in CPS.

### *Models of Cyber-Control Interface Dependencies.*

Cyber security properties are expressed in terms of the objectives of confidentiality, integrity and availability (CIA). CPS and their control systems are concerned with control-theoretic properties such as controllability, stability and observability (CSO). The research challenge is to formulate formal models and principles at the interface of the cyber and control layers so as to formally reason about how cyber attacks and CIA properties perturb CSO (and similar) properties and the physical operations of the CPS.

### *Attack Mitigation, Detection, Restoration and Recovery.*

A research challenge is to design strategies to mitigate, detect and triage attacks, as well as address restoration and recovery. Triaging attacks, and the restoration and recovery of the system should be mindful of mission priorities and impact. Not all attacks may need to be attended to in an urgent manner. Restoration and recovery needs to be sequenced carefully so that critical services are given the highest priority.

### *Security Maintenance.*

Patching on a regular basis is not viable in many CPS systems due to their high uptime requirements. To address this problem in the CPS context requires building a profile of a CPS so as to understand which parts of the system are active (i.e. hot) when and as well as which are inactive (i.e. cool). For example, a particular pump in a refinery may only become active once a week (say on a Sunday) during the weekly maintenance and flush routine. So the associated PLC controller may be patched at other times without interfering with mainstream operations.

### *Privacy.*

All new CPS deployments are meant to solve societal problems and improve our standards of living. Several of these CPS deployments however can capture personally sensitive data in the process and a big challenge is to design systems that achieve benefits to society while maintaining individual privacy expectations.