Incremental Security Enforcement For Cyber Physical Systems

Guide: Dr K. S. Sudeep

Aaditya. M, Lalit. N , V. Vijay, N. Karthik

Abstract

Cyber-Physical Systems (CPS) are increasingly prevalent in critical applications, from industrial automation to autonomous drones. These systems are vulnerable to cyber-physical attacks (CP-attacks) that exploit both cyber and physical components. Unlike traditional cyber systems, CPS lacks mechanisms to apply security patches incrementally, leaving them exposed to new threats. In this work, we propose a compositional runtime enforcement (RE) framework that enables the incremental addition of security policies as new vulnerabilities emerge, without affecting previously enforced policies. Using a case study of drone swarms, we demonstrate how our approach mitigates various attacks, including boundary breaches and conflicting control signals. Experimental results show that our method avoids state space explosion, maintaining a linear relationship between the number of policies and system performance, making it a scalable and efficient solution for enhancing CPS security.

Introduction

A comprehensive incremental security enforcement approach tailored for Cyber-Physical Systems (CPS), which aims to enhance security by incrementally integrating new security policies as new threats emerge. Unlike conventional security systems, CPS faces unique challenges due to its intertwined physical and cyber components, which make it vulnerable to cyber-physical attacks (CP-attacks). Existing runtime enforcement (RE) methods for CPS are not designed to handle the dynamic and evolving nature of these systems, leaving gaps when it comes to introducing new security patches without disrupting ongoing operations. The proposed model is organized around three key components of incremental runtime enforcement: Compositional Runtime Enforcement (CRE) and Policy driven Input/Output Enforcement. Through the implementation of these components, our model ensures enhanced security for CPS while maintaining system performance and avoiding issues such as state space explosion. Using drone swarms as a case study, we validate the effectiveness of our approach in mitigating CP-attacks, demonstrating its ability to enforce complex security policies incrementally and efficiently.

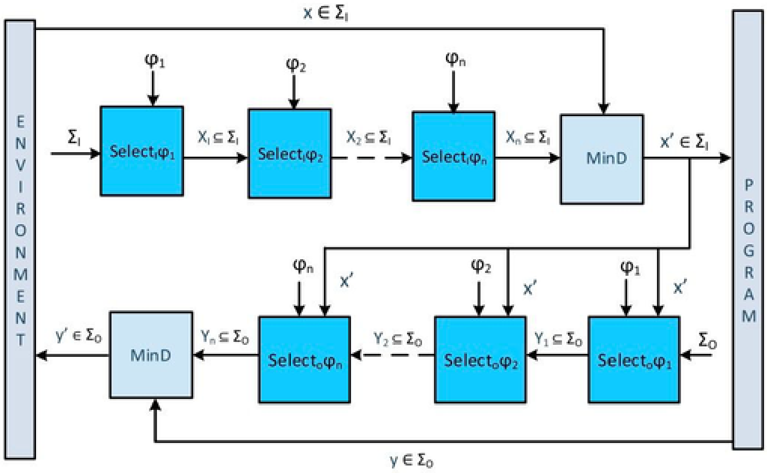
Methodology

The methodology for this incremental security enforcement project begins with the development of a bi-directional runtime enforcement (RE) framework, tailored to monitor and control both inputs and outputs in cyber-physical systems (CPS). This framework addresses the complex requirements of CPS, where new security policies must be incrementally added without triggering a complete overhaul of the system's enforcement structure. To manage the complexity associated with enforcing multiple security policies, the project applies two approaches: a monolithic enforcement model, which combines all policies into one, and a serial composition model, which enforces policies individually in sequence. The serial composition approach allows the addition of new policies without affecting the existing ones, thus preventing state-space explosion and maintaining efficient operation as the number of policies grows.

Algorithm

The algorithm for incremental security enforcement in cyber-physical systems (CPS) uses a serial composition of enforcers, each dedicated to enforcing a specific policy. These enforcers are linked sequentially, so the output from one serves as the input for the next, allowing new policies to be added without revalidating the whole system. Input and Output Enforcement Functions manage data flow by checking inputs for compliance before they enter the CPS and verifying outputs before they are released.

Edit and Select Functions handle any necessary modifications, ensuring inputs and outputs adhere to policies with minimal deviation from the original data. This Incremental Enforcement method enables real-time compliance by processing each event in sequence, providing a scalable and adaptable security solution for complex CPS environments.



Conclusion

As security policies evolve pertaining to security attacks in cyber-physical systems, its worth investigating how the security framework needs to adapt. The monolithic technique, in which the framework must be developed from scratch, does not appear to be efficient. In this work, we investigate the serial compositionality of runtime enforcers in response to the rise of new security policies. We consider the bi-directional enforcement mechanism in a synchronous reactive system. We propose an approach for the composition of enforcers in series. We show that using the proposed compositional framework, enforcers can be composed serially and can be used to enforce any set of policies that can be enforced using the monolithic approach. As a result, the suggested framework enables the gradual insertion of additional enforcement and security layers as needed (for instance, whenever a new security-related risk or issue arises) without affecting the policies that have already been in action.

References

Incremental Security Enforcement for Cyber-Physical Systems by ABHINANDAN PANDA , ALEX BAIRD, SRINIVAS PINISETTY, AND PARTHA ROOP; Scalable Security Enforcement for Cyber Physical Systems by ALEX BAIRD , ABHINANDAN PANDA , HAMMOND PEARCE , SRINIVAS PINISETTY , AND PARTHA ROOP; Monitoring and Defense of Industrial Cyber-Physical Systems Under Typical Attacks: by Yuchen Jiang , Shimeng Wu , Renjie Ma , Ming Liu , Hao Luo , and Okyay Kaynak