Formal Methods for Secure Cyber-Physical Systems Workshop: Report on the First Edition

James G. Wright
Department of Information Security
and Communication Technology
Norwegian University of Science
and Technology
Gjøvik, Norway
james.g.wright@ntnu.no

Stephen D. Wolthusen
Department of Information Security
and Communication Technology
Norwegian University of Science
and Technology
Gjøvik, Norway
Department of Information Security
Royal Holloway
Egham, United Kingdom
stephen.wolthusen@{ntnu.no,rhul.ac.uk}

***Abstract*—This position paper outlines the themes and challenges identified during an international workshop held on March 15, 2024 in Oslo, Norway on "*Formal Methods for Secure Cyber-Physical Systems*".**

The security of cyber-physical systems (CPS) has largely been considered as a straightforward extension of security problems in the computational domain. This abstraction, however, elides both constraints arising from the physical domain such as limits on what can be known about the internal state of the physical system, and also security and safety properties required to characterise the correct functioning of a CPS.

To advance research in this area, we argue that a rigorous shared family of adversary models and the development of these synthesized safety/security properties is highly desirable not only to render results comparable, but also as a pre-requisite for effective automation of verification and validation.

***Index Terms*—Cyber-physical systems, security properties, formal methods, adversary models**

I. Introduction

In this position paper we summarise the key themes arising during the *"Formal Methods fo Secure Cyber-Physical Systems (CPS)"* in March 2024, which was convened after discussions at an earlier seminar on formal methods at the University of Reykjavik in 2023.

Recent years have seen substantial advances in the formal methods community yet limited uptake in the security domain; at the same time the problem space of distributed systems which must also interact with physical environments has not been considered extensively by this community. CPS, moreover, will require not only safety properties, but also allow adversaries to interact so that the requirements of the operator are thwarted in ways that are poorly characterised by conventional security properties.

The workshop sought to identify the opportunities and challenges for collaborative research in this space and alighted on three inter-linked themes:

- Enhanced Fidelity Security Models for Cyber-Physical Systems
- A Family of Common Adversary Models for Cyber-Physical Systems
- Automation Challenges for the Verification of Cyber-Physical Security and Safety Models and Reasoning

In the remainder of this position paper we will briefly discuss each of the themes and conclude with a proposed roadmap with an emphasis on the research opportunities for the formal methods community.

II. Enhanced Security Properties for Cyber-Physical Systems

The security research community relies on a well-understood shared set of security properties for digital systems, although this typically excludes more granular notions of availability such as explicit time constraints that would be considered for safety or correctness of e.g. real-time and reactive systems.

What has largely been the preserve of the safety research community and disciplines adjacent to control theory are the limits of what can be known about the internal state of physical systems based on observability as well as constraints on the sensors such as precision and accuracy of these.

To reason over security properties of CPS, however, both domains must be integrated in a sufficiently granular manner since it is not only the omission of a given security property that may be problematic, but also when assumptions about the strength of a property is inappropriate.

As non-trivial CPS are likely to be distributed and composed of multiple, interacting elements, all of the above must also be *composed*, requiring a rigorous understanding also of

Funded by the Norwegian Research Council SFI NORCICS (310105).

the compositional properties of the security property classes outlined above.

All of the above, moreover, must adhere to a common semantic model, at least for a given instance, since it can be assumed that the security property (or rather violations thereof) will interact with one another.

III. Common Adversary Models for Cyber-Physical Systems

Closely related to the issues raised in the previous section, the verification CPS security properties is currently constrained by the ability to capture all adversarial behaviour, as well as the current focus on solely either local traces or a global trace requiring which leads to substantial simplifications.

More subtle adversarial behaviour models, however, require not only the ability to target the security properties highlighted in the previous section, but also (partial) orders over local traces when studying the fragility of local correctness in the face of an adversary who is capable of manipulating state and communication.

Alongside this both adversaries and defenders are limited in what they can know about the state of a cyber-physical component and, moreover, the entire system as they constrained by results from distributed systems. Verification models should therefore be able to impose restrictions on the local knowledge of adversaries, their ability to communicate including timeliness of communication, and also whether the adversary is able to explicitly sample the physical state of the CPS. These capabilities can be arranged hierarchically, which avoids the prospect of unintentional ad hoc assumptions being introduced when modelling CPS security.

We also note that adversary behaviour in a CPS would potentially affect the state of both the digital and physical domains, and particularly in the latter case in ways which may again not be possible to measure fully, resulting in added uncertainty also for adversaries in the causal model used by these.

IV. Automation of New Verification Models

Finally, building on the previous themes, we identify challenges faced by the automation of security proofs and verification of secure CPS. As noted above, one of the challenges faced in this domain is the problem of composability along with the expansion of semantics for required new adversarial equational theories representing the limitations of capabilities and knowledge as well as suitable representation of the CPS. Even individually, these would likely overwhelm the limits of current automated verification systems. The ability to state the limits of properties, within the various configurations of distributed systems, formally is hence a desideratum in its own right.

Two aspects requiring explicit formalisation for automation are bounds on the adversary's memory (i.e. ability to learn) and abilities (i.e. temporal accuracy of their manipulation), and to what extent the CPS properties can be formalised; which can build upon the extensive research in the verification of hybrid and reactive systems.

V. Proposed Directions

The issues highlighted in this position paper were presented in a sequence that fits naturally with a process of consensus-building in the community; hence the proposal for creating an explicit working group which co-ordinates activities since the alternative of ad-hoc activities would be slow and inefficient; we also believe that this area can be considered amenable to co-operation since it affords greater comparability of results and should help avoid duplication of effort in this problem space.

A further issue is the identification of suitable venues that allow participation from the adjacent research communities to interact; this is currently an imperfect match at best that skews to particular domains. Research areas with such limited representation would e.g. include

- CPS security models with explicit time and reliability notions.
- Adversary models for CPS grounded and informed by control theoretical and distributed systems results
- Synthesis of methods from the security formal methods, hybrid and reactive systems communities.

The authors welcome engagement by members of the relevant communities and look forward to moving this important domain forward.