ABSTRACT

Advances in the interconnected capabilities of cyber physical systems (CPS) affect virtually every engineered system. Today, software approaches dominate all aspects of connecting the physical and cyber worlds in part due to the convergence of computing, control and communications software technologies. Unfortunately, software technologies are more vulnerable to cybersecurity problems than traditional hardware solutions. This workshop aims to develop a research agenda for engineering cybersecurity into cyber physical systems (CPS) through design-time requirements engineering, continuous assurance at runtime, and cognitive security analytics.

CPS are distributed, software-intensive smart systems that control tightly integrated computational and physical components. A combination of design-time and runtime techniques are needed to support reasoning about cybersecurity. We advocate a holistic requirements engineering approach, continuous validation with feedback loops supported by models at runtime and networked control, and cognitive security analytics using Watson.

CCS Concepts

• Software and its engineering→Software organization and properties→Software system structures
• Security and privacy→Software and application security→Software security engineering

Keywords

Cybersecurity; cyber physical systems (CPS); Internet of Things (IoT); engineering cybersecurity; cognitive security analytics; holistic requirements engineering; continuous assurance; models at runtime (MART); networked control.

1. INTRODUCTION

Cyber physical systems (CPS) are distributed, software-intensive systems that control tightly integrated and networked computational and physical components [1][2][3][4][5][6]. The societal impact of CPS and its associated industrial revolution is enormous. CPS technologies are becoming the key enablers for how we control and build smarter, context-aware and situation-aware systems, such as autonomous vehicles, smart cities and buildings, renewable energy systems, elderly healthcare, resource management, and food supply chains [7][8][9][10][11][12].

Cybersecurity is a key concern in all of these application domains [13][14][15][16][17][18]. There are many challenges that must be addressed in engineering CPS. CPS are often engineered as systems of systems. Some of these subsystems—physical and computing subsystems—have been engineered before cybersecurity was a global and pervasive concern. The goal of this workshop is to bring together researchers from different fields to develop a research agenda for engineering cybersecurity into cyber physical systems.

At the core, CPS are adaptive systems [19] where computing components control and augment physical components. Adaptive systems are engineered using models at runtime as a foundation for reasoning [20][21][22][23][24][25], feedback loops implemented as networked control systems to manage CPS capabilities [26][27][28][29][30][31][32][33], and continuous assurance algorithms to validate requirements at runtime [34][35]. One the one hand, these subsystems must be protected against cybersecurity threats. On the other, we posit that the capabilities of these adaptive system components can be exploited to engineer actionable cybersecurity properties into cyber physical systems.

2. DEFINING CYBERSECURITY

Cybersecurity can be at risk, and the degree of interconnection of those elements can make it difficult to determine the extent of the cybersecurity framework that is needed [13][14].

There are many related cybersecurity definitions. The Investment Industry Regulatory Organization of Canada features the NIST and ISO definitions in their recent Cybersecurity Best Practices Guide [15][18].

NIST: The National Institute of Standards and Technology (NIST) defines cybersecurity as “the process of protecting information by preventing, detecting, and responding to attacks.” Similar to financial and reputational risk, cybersecurity risk affects a company’s bottom line. It can drive up costs and impact revenue. It can harm an organization’s ability to innovate and to gain and maintain customers [16].

ISO: The International Organization for Standardization (ISO) defines cybersecurity as “the preservation of confidentiality, integrity and availability of information in cyberspace where cyberspace is the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form” [17].

3. CYBERSECURITY REQUIREMENTS

Van Lamsweerde argues that caring for security at requirements engineering time is a message that has now traction and is a key concern in the software industry [36]. Frameworks are emerging to facilitate the engineering of requirements for reliability and security [37].
CPS are socio-technical ecosystems involving people, processes, technology, and infrastructure. Frequently, CPS are designed in a piecemeal rather than a holistic fashion, leaving parts of the system vulnerable. Mylopoulos et al. propose a holistic requirements engineering approach to deal with the challenges of socio-technical ecosystems [38]. Their approach features a three-layer security analysis framework consisting of a social layer (business processes, social actors), a software layer (software applications that support the social layer), and an infrastructure layer (physical and technological infrastructure) to structure the design of digital ecosystems. In their proposal, global security requirements lead to local security requirements, cutting across requirements analysis across the three layers. They also propose a set of analytical methods and a systematic process that together drive security requirements analysis across the three layers.

4. ASSURANCE AT RUNTIME

One of the characteristics of a cyber physical system is that it modifies its own behavior at runtime in response to changes within its computing subsystems or within its physical subsystems [39]. Thus, not only the fulfillment of the system requirements needs to be guaranteed in the presence of adaptations at runtime, but also the response to cybersecurity threats and attacks must satisfy requirements. Thus, a key challenge for CPS is continuous assurance at runtime. Traditionally, confidence in the correctness of a system is gained through a variety of activities and processes performed at development time, such as design analysis and testing. In the presence of self-adaptation or disturbances, some of the assurance tasks need to be performed at runtime. Cybersecurity attacks can be viewed as disturbances affecting the running system.

This need calls for the development of techniques that enable continuous assurance throughout the software life cycle [39][40][41]. Research is needed to understand what information needs to be captured by models at runtime (MART), specifically for the purpose of assurance.

5. COGNITIVE SECURITY

In a white paper on cognitive security [42], IBM advocates to employ cognitive systems to analyze security trends and distill enormous volumes of structured and unstructured data into information, and then into actionable knowledge to enable continuous security.

Cyber physical systems inherently include several capabilities required to enable cognitive security. CPS are naturally instrumented to monitor the context of components, processes and the environment using feedback loops and controllers operating on MART.

In CPS, the analytics engine typically analyzes patterns and the planner decides on how to adjust variables. Engineering cognitive security into CPS involves monitoring relevant information, analyzing this massive amount of information and its context using an advanced analytics engine, such as Watson, and deciding how to react to perceived security threats. Watson could detect deviations from regular patterns, uncover changes in network traffic, and identify irregular activities [42]. Traditional CPS MART have to be extended to accommodate the cognitive security models.

6. CONCLUSIONS

To reap the benefits of the CPS revolution, it is imperative to invest in cybersecurity research that spans the CPS foundations—computing, control and communications. We posit that ensuring or enforcing cybersecurity properties requires not only using design-time requirements engineering and static analyses, but also through continuous validation and assurance with feedback loops supported by models at runtime, networked control, and cognitive security analytics.

7. ACKNOWLEDGMENTS

This work has been funded in part by University of Victoria, York University, and University of Toronto, Canada; and by NSERC Strategic Research Network for Smart Applications on Virtual Infrastructure (SAVI-NETGP 397724-10).

REFERENCES
