Designation of Critical Cyber-Physical Systems Software: From Research to Practice

Sandip Roy, Program Director, Computer and Information Sciences and Engineering Directorate, United States National Science Foundation, (Contact: saroy@nsf.gov)

Background and Scope: The United States National Science Foundation (NSF) has persistently invested in computer security research over a multi-decade period. Today, the NSF supports a substantial and diverse portfolio in cyber-security through a number of programs and solicitations, such as Secure and Trustworthy Cyberspace (SaTC), Cyber-Physical Systems (CPS), and Cybersecurity Innovation for Cyberinfrastructure (CICI). This portfolio spans the technological and socioeconomic dimensions of cybersecurity research; encompasses software, systems, and data security; and engages partners including other federal agencies, state and local governments, and private industry at both the program and project levels.

Within the NSF cybersecurity ecosystem, there has been a particular focus during the last few years on cyber-physical systems (CPS) security. Holistically, CPS security work is concerned with protecting from attack and making resilient engineered systems with embedded cyber (computing, communications, control) components. CPS requiring security solutions range from terrestrial-scale infrastructures like the bulk power grid and the air transportation system, to Internet-of-Things deployments at the building or neighborhood scale, and to small-scale sensing-actuation systems like smart watches or even bloodstream glucose sensors. Given the pervasive reliance on cyber technologies for engineered systems at all scales, it is not surprising that many recent high-impact cyber- attacks have been concerned with embedded rather than stand-alone computing and software systems, i.e. CPS. Indeed, the Executive Order (EO) on Improving the Nation's Cybersecurity (14028) directly followed a ransomware attack on the Colonial Gas Pipeline which incurred far-reaching effects on the physical infrastructure (specifically, resulting in a shutdown of the pipeline), and responds to several other attacks which had prominent signatures in the engineered world (e.g., dumping of chemicals into water distribution systems, power outages, airport closures).

The purpose of this position paper is to call to attention the importance of CPS security research in addressing the pressing cyber-security challenges identified in the EO, including efforts to secure software supply chains. The position paper focuses particularly on identification and designation of critical software (Workshop Topic 1) in cyber-physical systems. Specifically, a rationale is given for why ongoing CPS security research is relevant to critical software designation (**Relevance of CPS Security Research)**. On this basis, the position paper then advocates for drawing on the body of CPS security research to develop criteria for designating CPS software as critical in the short term, and enable systematic evaluation of criticality in the longer term (**Translating Research to Practice)**.

Relevance of CPS Security Research: The complex integration of heterogeneous software within physical-world engineered systems creates challenges in securing their supply chains, including in designating which software components are critical. In particular, determining which software components are critical – i.e. both vulnerable to intrusion and causative of systemic failures upon attack – is especially challenging in the CPS space because of their complex interdependencies with other physical/cyber components and their complex provenance.

Ongoing CPS security research has had several foci which are germane to designating embedded software components as critical, for the purpose of software supply-chain security:

1) *Threat impact analyses,* wherein compositions of multiple cyber and engineered components are modeled in tandem, and implications of component-level failures/attacks on holistic CPS functions are assessed. These impact analyses indicate interdependencies between a software component and other components, and allow evaluation of the potential harm to overall system functions due to an attack on a component, which are needed for determining criticality of software components.
2) *Life-cycle management for CPS and IoT,* which recognizes the complex provenance and evolution of embedded software. This research has potential to yield techniques for determining the evolving vulnerability of embedded software to cyber threats throughout its life-cycle, including vulnerabilities introduced during production and distribution, which is important for distinguishing critical software.
3) *Security for human-in-the-loop CPS,* which encompasses design of trustworthy software and systems, and evaluation of threat impacts when operators/clients are part of the system. These efforts are yielding additional techniques and refined constructs for understanding the potential impacts of cyber threats, which can support designation of critical components.
4) *Inter-disciplinary and holistic project scopes,* which include domain experts along with computer and information scientists, consider security as part of a broader set of objectives (including system functionality, performance, safety, and resilience), and often merge industry and academic viewpoints. These integrative approaches and teams have the wherewithal to effect practical changes and gain credence in domains where software security is traditionally a secondary consideration.

Translating Research to Practice: Although CPS security research and development is in its nascency (in the main less than 10 years old), we believe that it is an important asset in the designation of critical cyber-physical software, as part of the broader effort to secure software supply chains. The EO envisions the formulation of criteria for designating software as critical over a very short time horizon (45 days), Even during this very short horizon, we advocate for drawing on the body of research on CPS security, to assist in formulating criteria for embedded or CPS software. Specifically, via the research foci described above, CPS security research is elucidating the heterogeneous factors which influence threat susceptibility and impact, and providing quantitative metrics for these various factors. We anticipate that the identified factors will be helpful in developing an encompassing definition, which is credible to system operators. Over a longer term (~1-5 years), the CPS research outcomes can be translated into quantitative measures and criteria for the criticality of software components. Additionally, CPS models and methods can be transitioned into practical decision-support tools for assessing the vulnerability of critical software components to cyber-attacks, and evaluating holistically the potential harm caused by these potential attacks. A number of ongoing efforts in the CPS research community, including federal working group activities, workshops, and academic-industry partnerships, are supporting transition of research outcomes on CPS security into such practical guidelines and operational tools for system security. We strongly believe that engaging the CPS security community in developing guidelines for security, as envisioned by the EO, will help to foster the development of scalable and credible cybersecurity solutions.