Testing Requirements and Approaches for Software Embedded in Next-Generation Critical Infrastructures

Sandip Roy (sandip@wsu.edu) and **Haipeng Cai**, Washington State University
Mengran Xue, Raytheon BBN Technologies

Scope: The past few years have witnessed an increasing frequency of high-profile cyber- attacks on critical infrastructures, including attacks on the Colonial natural-gas pipeline and on the Oldsmar, Florida water distribution system earlier in 2021. These cyber-attacks on critical infrastructures have the potential to incur tremendous costs in terms of infrastructure damage, lost productivity, and human morbidity and mortality, because they have propagative impacts on physical-world processes that are foundational to modern communities. For instance, the attack on the Florida water distribution system temporarily increased sodium hydroxide input into the water system, which if left unchecked could have caused severe illness. At the same time, critical infrastructures are evolving from siloed systems to highly networked *next-generation systems* with Internet-Protocol back-ends, pervasive sensing, and distributed automation. In consequence, infrastructures today have a greatly magnified cyber- attack surface, i.e. they are susceptible to diverse attack modalities from many potential intruders as well as highly varied failure modes. The growing susceptibility and potential cost of cyber-attacks on next-generation critical infrastructures dictates that standards and methodologies are needed for design, procurement, testing, and maintenance of their software, as encompassed by the Executive Order (EO) on Improving the Nation's Cybersecurity (14028). This position paper focuses particularly on requirements and approaches for testing software embedded in next-generation critical infrastructures (Workshop Topic 4).

The position paper's authors are a part of a team of academic and industry researchers who have been involved in cyber-security and cyber-risk management work in multiple critical infrastructure sectors. Here, we firstly describe our experiences in some of these domains with the goal of highlighting a common need for nimble integrative testing of embedded software (**Experiences**). The position paper then identifies key challenges which must be accounted for in developing requirements for software testing (**Challenges)**. Finally, we highlight a few technologies which are promising for meeting these integrative software-testing requirements for next-generation critical infrastructures (**Promising Technologies**).

Experiences: The position paper's authors have been engaged in methodological research and tool development for assessment/mitigation of cyber-threats to several next-generation critical infrastructures, as well as domain-agnostic research on security testing for large-scale distributed software systems. Here, we briefly describe our efforts in a couple of domains, to motivate integrative software testing approaches for software embedded in critical infrastructures.
Threat Assessment for the Next-Generation Air Transportation Systems: During the last 5-7 years, the U.S. air transportation system has been impacted by a number of software failures and breaches which caused system-wide flight delays and cancellations. In response to these incidents, recent studies from our group and others have sought to model the propagative impacts of intrusions/failures on aviation-system performance [1]. Our interactions with operators and domain scientists in this context have indicated a glaring need for comprehensive evaluation of system software from a security perspective. In addition, practitioners crucially need tools for

assessing the interdependencies among software systems, and between software and physical-world systems, as new cyber technologies are brought online.
Cyber-Risk Management in Next-Generation-911 Systems: The emergency communications system in the United States is being transitioned to an IP-based next-generation infrastructure, which can provide significant benefits in terms of access (e.g., Voice-over-IP 911 calls, image/video transmission) and resilience (e.g. via automated rerouting of calls or dispatch during disasters). The growing interconnectivity of the emergency communication system, however, is leaving it susceptible to cyber-threats which can have substantial impact on resource availability and service times. This has motivated several research and development efforts, often led by small businesses, to assess and mitigate cyber-security risks to NextGen 911 systems (see [2] for our effort on risk assessment using cyber-physical queueing network models). These efforts are calling to attention the need for both real-time and design-time testing of the interdependent software and physical-world components of emergency response systems.
Software-Testing Foundations: Current research is focused on developing scalable and cost-effective software code analysis techniques for dynamic security testing, such as tracking run-time information flow and discovering security vulnerabilities, in networked and distributed systems [1]. These methods address the complex interdependencies and myriad attack modalities in large-scale distributed systems.

Challenges: Although the software systems embedded in different critical infrastructures are widely varied, security testing entails several common challenges which reflect the enormous sophistication of these systems. First, the software systems are interdependent with each other and with physical processes as well as human operators/clients, which means that intrusions may have propagative impacts across the cyber-physical-human infrastructure. Second, software for next-generation infrastructures is extremely heterogeneous in their provenance and specifications, and managed in a decentralized way by heterogeneous stakeholders. Third, the operational drivers and environments of large-scale infrastructures are constantly varying. Fourth, as infrastructures are pervasively sensed and networked, and also customized/ democratized, their attack surfaces are becoming very large. We advocate that testing requirements, as solicited in the EO, must be integrative (i.e. capturing interdependencies, heterogeneity, and system and attack diversity) to account for these challenges.

Promising Technologies: The following are a few technologies which we believe can assist in integrative testing of software embedded in critical infrastructures, by helping to address the challenges listed above: 1) *Cyber-Physical-Human Digital Twins* which allow plug-and-play testing of software within a framework which represents component interdependencies across the infrastructure; 2) *Critical-Points Analyses* based on abstracted models and network analytics, to focus testing on critical software components and attack modalities. 3) *Lightweight Dynamic Testing* to enable cost-effective and timely response to evolving attacks and moving targets, through self-adaptation and on-the-fly attack detection. Such strategies continuously learn from the dynamic environment and adjust defense algorithms automatically to sustain scalable and cost-effective protection of the systems under testing.

[1] A. Tamimi, A. Hahn, A, and S. Roy. “Cyber Threat Impact Analysis to Air Traffic Flows Through Dynamic Queue Networks”. *ACM Transactions on Cyber-Physical Systems*, *4*(3), 1-22, 2020.
[2] M. Xue and S. Roy, ``Cyber-Physical Queueing-Network Model for Risk Management in Next-Generation Emergency Response Systems.” *arXiv:2101.11198*.
[3] X. Fu and H. Cai. “FlowDist: Multi-Staged Refinement-Based Dynamic Information Flow Analysis for Distributed Software Systems”. In: 30th USENIX Security Symposium (USENIX Security 21). 2021.