Software plays a critical role in computing systems, including cyber-physical systems such as drones. Unfortunately, understanding complicated software systems is challenging, resulting in insecure and vulnerable systems. A fundamental challenge for security analysis of modern systems is handling overwhelming complexity and dependencies among the software components. In this talk, we will walk through two systems dealing with complex software systems to improve the security of the systems: (1) finding logic flaws and (2) fixing configuration bugs of drone swarm algorithms. Specifically, I will demonstrate how a complex drone swarm's behavior can be systematically measured and understood, eventually guiding a greybox fuzz testing to effectively test diverse behaviors of drone swarms and discover logic flaws. I will introduce the novel interpretation of counterfactual causality in the context of robotics. With the system, we find 42 unique mission failures, 15 root causes, and 15 potential fixes confirmed by developers. Further, I will show how we can leverage the counterfactual causality to fix configuration bugs (i.e., bugs caused by misconfiguration of the swarm algorithm).

Biography

Dr. Yonghwi Kwon is an assistant professor of ECE (Electrical & Computer Engineering) at the University of Maryland. He is broadly interested in solving system security problems via program analysis and counterfactual causality inference. He is a recipient of the NSF CAREER and CRII Awards, two ACM Distinguished Paper Awards, and two Best Paper Awards in Automated Software Engineering (ASE) and WISA. Previously, he also won the championship of the National CCDC (Collegiate Cyber Defense Competition) in 2019 and 2020 as a team coach.