Prototype pollution is a relatively-new type of vulnerability specific to prototype-based languages, such as JavaScript, which allows an adversary to pollute a base object’s property, leading to further consequences such as Cross-site Scripting (XSS) and session fixation. In this talk, I am presenting our research works in the past five years, which detect and exploit not only prototype pollution vulnerabilities but also other related JavaScript vulnerabilities across server-and client-side applications. I will start from our ESEC/FSE’2021 paper, which is flow- and context-sensitive JavaScript static analysis with hybrid branch-sensitivity and points-to information to generate a novel graph structure, called Object Property Graph (OPG), using abstract interpretation. Then, I will present our improved graph, called Object Dependence Graph (USENIX’2022), in detecting a wide range of JavaScript vulnerabilities and our dynamic analysis (NDSS’2022) in exploiting prototype pollution vulnerabilities in real-world websites. Lastly, I will briefly introduce our recent progress (IEEE S&P’2023 and CCS’2023) in scaling JavaScript abstract interpretation. Our JavaScript works discovered over 450 Node.js vulnerabilities with 102 CVE identifiers, 2,738 vulnerable websites, and 43 vulnerable browser extensions in total over the years.
paper nomination at CCS’20. He is a recipient of the DARPA Young Faculty Award (YFA) 2022, the Amazon Research Award 2021 and 2017, and NSF CAREER Award 2021.