Handling Large-Scale Volumetric DDoS Attacks with Trusted Hardware

KANG Min Suk

Assistant Professor

National University of Singapore

ABSTRACT

In light of ever-increasing scale (e.g., million-node IoT bots) and sophistication (e.g., amplification) of modern DDoS attacks, we argue that it is time to revisit one of the oldest, possibly most effective DDoS defenses --- source filtering or the idea of installing traffic filtering nearer to attack sources. Despite its fundamental benefits (e.g., cost-optimal filtering location, larger defense capacity) over other defense approaches (e.g., cloud-based scrubbing), source filtering remains an academic curiosity, and has never been widely adopted. A key reason that has stifled adoption is the lack of trust between ISPs --- that is, source and destination networks often have no existing relationships. In this talk, we show the technical feasibility of bootstrapping this trust between arbitrary source and destination networks by designing an auditable filter that enables the DDoS victim to check the correct filter operations executed in a remote source network. We utilize a recent trusted computing hardware platform, Intel SGX, as a feasible root of trust. Our proof of concept demonstrates that one auditable filter can handle nearly 10 Gb/s traffic and execute up to 3,000 filter rules. For larger attack volume (e.g., 100 Gb/s) and complexity (e.g., 50,000 filter rules), we propose an efficient filter rule distribution algorithm for dynamically (e.g., every 5 seconds) re-configuring large numbers of parallel SGX-based filters.

SPEAKER BIOGRAPHY

Min Suk is an Assistant Professor of Computer Science Department, School of Computing at National University of Singapore. His research interests lie in the field of network and distributed systems security, wireless network security, and Internet privacy. He obtained his PhD degree in Electrical and Computer Engineering from Carnegie Mellon University in 2016 under the supervision of Virgil D. Gligor in CyLab. He received BS and MS degrees in EECS at Korea Advanced Institute of Science and Technology (KAIST) in 2006 and 2008, respectively.