A Knights Welcome To: Min Suk Kang

DATE: Monday December 10, 2018

TIME: 10:30am-11:30am

LOCATION: R1-307

(Research I Building)

HOSTED BY: Aziz Mohaisen

Bio: 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 blockchain security. 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.

"Challenges in DDoS Defense and a New Approach with Trusted Hardware"

Large botnet-based Distributed Denial-of-Service (DDoS) attacks have recently demonstrated unprecedented damage. However, the best-known end-to-end availability guarantees against flooding attacks require costly global-scale coordination among autonomous systems (ASes). A recent proposal called routing around congestion (or RAC) claimed to provide strong end-to-end availability to a selected critical flow. In the first part of the talk, we will present our recent in-depth analysis of the (in)feasibility of the RAC defense. We show a fundamental trade-off between the two necessary properties of the proposed RAC defense, and as a result, the RAC defense is not just ineffective but nearly unusable in practice. In the second part of the talk, we will present a highly effective new approach to DDoS defense --- a secure in-network filtering or the idea of empowering DDoS victims to install in-network traffic filters in the upstream transit networks. We argue that all existing in-network filtering ideas are impractical due to the lack of verifiable filtering --- no one can check if the filtering service executes the filter rules correctly as requested by the DDoS victims. We show the technical feasibility of verifiable in-network filtering, called VIF, that offers filtering verifiability to DDoS victims and neighbor ASes. Our large-scale simulations of two realistic attacks (i.e., DNS amplification, Mirai-based flooding) show that only a small number (e.g., 5–25) of large IXPs are needed to offer the VIF filtering service to handle the majority (e.g., up to 80–90%) of DDoS traffic.