Public Abstract
First Name:Roshan
Middle Name:Lal
Last Name:Neupane
Adviser's First Name:Prasad
Adviser's Last Name:Calyam
Co-Adviser's First Name:
Co-Adviser's Last Name:
Graduation Term:FS 2017
Department:Computer Science
Degree:MS
Title:DOLUS: CYBER DEFENSE USING PRETENSE AGAINST DDOS ATTACKS IN CLOUD PLATFORMS

Cloud-hosted services are being increasingly used in online businesses in e.g., retail, healthcare, manufacturing, entertainment due to benefits such as scalability and reliability. These benefits are fueled by innovations in the orchestration of cloud platforms that make them totally programmable as Software Defined everything Infrastructures (SDxI). At the same time, sophisticated targeted attacks such as Distributed Denial-of-Service (DDoS) are growing on an unprecedented scale threatening the availability of online businesses. In this thesis, we present a novel defense system called Dolus to mitigate the impact of DDoS attacks launched against high-value services hosted in SDxI-based cloud platforms. Our Dolus system is able to initiate a pretense in a scalable and collaborative manner to deter the attacker based on threat intelligence obtained from attack feature analysis in a two-stage ensemble learning scheme.
Using foundations from pretense theory in child play, Dolus takes advantage of elastic capacity provisioning via quarantine virtual machines and SDxI policy co-ordination across multiple network domains. To maintain the pretense of false sense of success after attack identification, Dolus uses two strategies: (i) dummy traffic pressure in a quarantine to mimic target response time profiles that were present before legitimate users were migrated away, and (ii) Scapy-based packet manipulation to generate responses with spoofed IP addresses of the original target before the attack traffic started being quarantined. From the time gained through pretense initiation, Dolus enables cloud service providers to decide on a variety of policies to mitigate the attack impact, without disrupting the cloud services experience for legitimate users. We evaluate the efficacy of Dolus using a GENI Cloud testbed and demonstrate its real-time capabilities to (a) detect DDoS attacks and redirect attack traffic to quarantine resources to engage the attacker under pretense, and (b) coordinate SDxI policies to possibly block DDoS attacks closer to the attack source(s).