Application-Based DDoS Attack Prevention and Detection in Distributed Systems

Toktam Ramezanifarkhani, Elahe Fazeldehkordi, and Olaf Owe[2]

Department of Informatics, University of Oslo, Oslo, Norway

Abstract

Denial of Service (DoS) attacks and Distributed DoS (DDoS) attacks with even higher severity are historically considered among the major security threats and the hardest security challenges. Although there are lots of proposed defense mechanisms at the network to the application layers to overcome such attacks, based on recent experiences in 2016 and 2017, DoS and DDoS attacks are making the headlines frequently and have become the hugest cyber-attacks.

In this paper, our aim is to develop an additional layer of defense in distributed object systems to combat such threads by decreasing the attack damage and impact. We consider a high-level imperative and object-oriented framework based on the actor model with support of asynchronous and synchronous method interaction, which are popular and sophisticated features applied in many systems today while currently the non-distributed settings have been considered and analyzed in related work. We provide a hybrid approach including static and dynamic phases. In the static phase, we identify and prevent potential vulnerabilities in asynchronous communication that can cause flooding interactions between objects triggered from inside or outside of the system leading to DoS or DDoS attacks. For the dynamic phase, we also instrument the program to detect any possible remaining threads at runtime.

Keywords: DDoS Attacks, DoS Attacks, Flooding Attacks, Distributed Systems, Static Analysis, Trace Analysis.

[1]SCOTT (www.scott-project.eu) has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737422. This Joint Undertaking receives support from the European Unionâs Horizon 2020 research and innovation programme and Austria, Spain, Finland, Ireland, Sweden, Germany, Poland, Portugal, Netherlands, Belgium, Norway.

[2]email: {toktamr,olaf,elahefa}@ifi.uio.no