Kübra Kalkan
Thesis Supervisor: Prof. Fatih Alagöz

FILTERING BASED DEFENSE MECHANISMS AGAINST DDOS ATTACKS FOR CORE NETWORKS

Abstract

In this thesis, we present filtering based defense mechanisms against Distributed Denial of Service (DDoS) attacks for core networks. Initially, several filtering techniques are analyzed and their advantages and disadvantages are presented. A comparative classification of these methods is provided for security analysts. Classification results suggest that there are a few filtering methods that are both proactive and collaborative. Proactivity provides prevention of attacks before it spreads whereas collaboration enables getting knowledge about different points of the network and deciding filters together. Thus, we proposed a proactive and collaborative model called ScoreForCore. It is a statistical packet based defense mechanism that selects the most appropriate attributes for current attack traffic. Our results suggest that the success of the system's behavior on legal and attack packets increased considerably. This strategy is also convenient for current emerging technology for core networks, called Software Defined Networking (SDN). It has several problems related to security that are largely induced by the centralized control paradigm. In that regard, DDoS attacks are specifically valid for SDN environment. Several defense mechanisms in SDN environment are analyzed and comparative classification is provided for rendering the current state of the art in the literature. Then, our defense strategy is applied on SDN environment with capable switches. This mechanism's(SDNScore) results suggest that it gives perfect results for several known attacks and 84% success for an unknown attack. Since there is a trade-off between SDN paradigm and capable switches in SDNScore, we improved it and proposed another model called Joint Entropy based Scoring for SDN (JESS) that carries all burden to the controller and does not need capable switches. The results suggest that it is an elegant defense method for SDN environment.

PUBLICATIONS

Journals

1. **Kalkan, K.** and Alagöz, F. "A distributed filtering mechanism against DDoS attacks: ScoreForCore." Computer Networks 108 (2016): 199-209, 2016.
2. **Kalkan, K.**, Gür, G., Alagöz, F., "Filtering Based Defense mechanisms against DDoS Attacks: A Survey", accepted by IEEE Systems Journal, 2016.
3. **Kalkan, K.**, Gür, G., Alagöz, F., "Defense Mechanisms Against DDoS Attacks on SDN Environment", submitted to IEEE Communications Magazine, 2016.
4. **Kalkan, K.**, Altay, L., Gür, G.,Alagöz, F., "Joint Entropy based Scoring against DDoS attacks in SDN environment: JESS", in progress for submission to IEEE/ACM Transactions on Networking, 2016.

Conferences

1. **Kalkan, K.**, Gür, G., Alagöz, F., "SDNScore: A Statistical Defense Mechanism Against DDoS Attacks in SDN Environment", submitted to IEEE ICC 2016, Paris, France, 21-25 Mayıs 2017.

Defense Jury Members

1.	Prof. Fatih Alagöz	Boğaziçi University
2.	Prof. M. Ufuk Çağlayan	Boğaziçi University
3.	Prof. Albert Levi	Sabancı University
4.	Prof. Sema Oktuğ	İstanbul Technical University
5.	Prof. Tuna Tuğcu	Boğaziçi University

Defense Date: 07.10.2016