Chapter 11

GCD: A Global Collaborative Defense Approach to Thwart Internet Attacks

Subrata Acharya
Towson University, USA

ABSTRACT

With the tremendous growth in the dependence of services on the Internet, service disruption has become less and less tolerable. The greatest threat to service availability is the rapid growth in the complexity and frequency of large-scale distributed attacks. These attacks cause economic losses due to unavailability of services and potentially serious security concerns by the incapacitation of critical infrastructures. Despite the tremendous attention by the research community to find distributed attack countermeasures, a practical and comprehensive solution is yet to see the light of the day. In this research, the authors present a research direction aimed at finding a solution to the above problem.

INTRODUCTION

It is well understood that it is difficult to eliminate all distributed attacks, as it would require securing all machines on the Internet against misuse, which is not a economically feasible solution. A possible practical approach is to design defense mechanisms that will detect the attack and respond to it by dropping the excessive malicious traffic. These mechanisms will incorporate tools and mechanisms to comprehend the situational awareness information for such network systems. Generally, it is very easy to detect the distributed attack near the destination; however this is too late in attack detection. In the ideal case, the attack should be mitigated as close to the source as possible, but with the distributed nature of the attack it is not possible to decipher such attack with the little information available near the source of the attack. Additionally, the attack source is distributed in nature. Thus, a realistic solution should move away from single-point and local solutions towards a global and collaborative approach of attack detection and subsequent attack mitigation. To this effect this research presents the Global Collaborative Defense approach to detect and mitigate Internet attacks.

DOI: 10.4018/978-1-4666-0104-8.ch011
Distributed attacks are a serious threat to establishing and maintaining the stability and reliability of the Internet. To be specific, a DoS attack (Denial of Service Attack 2011) is an explicit attempt to interrupt an online service by generating a high volume of malicious traffic. These attacks consume all available network resources, thus rendering legitimate users to face service disruptions. The impact of the attack can vary from minor inconvenience to the users of a website, to serious financial loss to companies that rely on their on-line availability to do business (Mirkovic et al. 2002), (Papadopoulos et al. 2003).

Recent massive Internet worm outbreaks such as Slammer (Moore et al. 2003), Blaster (Symantec Security Response 2003) or Sasser (Symantec Security Response 2004) have shown that a large number of hosts (Lemos 2004) are patched lazily or are operated by security unaware users. Such hosts can be compromised within a short time to run arbitrary and potentially malicious attack code transported in a worm or virus or injected through installed back-doors. DDoS (Distributed Denial of Service 2011) use such poorly secured hosts as attack platform and cause degradation and interruption of Internet services, which result in major financial loss, especially if commercial servers are affected (Dubendorfer et al. 2004).

Keeping a commercial server available round the clock is a tough task; while attackers are able to exploit the processing and bandwidth resources and the flexibility of a huge number of compromised hosts to construct new attack tools and variants; operators of Internet servers are left without appropriate means to counteract attacks. Widespread availability of attack tools makes it trivial for naive users to carry out large-scale attacks. As a consequence, new attacks appear frequently, while defense strategies lag far behind. We believe that current security technologies and concepts that focus on end-system and access-networks are not able to cope with the growing number and the increasing intensity of these Internet attacks. Hence, it is evident that large-scale attacks can only be efficiently handled by providing increased security within the core network.

This motivates the need for robust, scalable and effective approaches for detecting and mitigating such attacks. Any effective and realistic solution should not add significant complexity in the core routers and should exhibit characteristics that allow it to scale to large network sizes and to handle large-scale distributed attacks. Also, the attack defense infrastructure should possess mechanisms to aid collaborative operation and be able to easily adapt to the traffic dynamics of the network. Most importantly such a solution should enable ease of security policy enforcement while maintaining and preserving the semantic integrity of the policy set. Finally, the proposed solution should not require considerable changes in the existing infrastructure in order to ease deployment in such large-scale networks. Thus, in this research we focus on a clean-slate approach and argue for a separate security plane to detect and mitigate distributed attacks. The decision logic for the security mechanisms is distributed in a small set of active security guards (Active sentinels), each responsible for a set of core routers. The Active sentinels collaborate both by proactive and reactive mechanisms to mitigate attacks. In section 3 we present although discussion of the proposed collaborative defense model aimed at limiting distributed attacks.

**BACKGROUND AND MOTIVATION**

The phenomenal success of the Internet is primarily attributed to the *end-to-end* principle (Saltzer et al. 1984) and the notion of core routers as dumb transmission systems, which enables fast transmission and best-effort delivery. Unfortunately, the success also encompasses the inborn limitations of the Internet, i.e. Security (policing) and QoS (reliability, rate control).