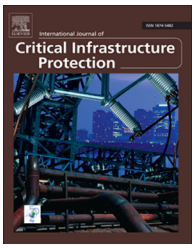
Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.elsevier.com/locate/ijcip



Analysis of the effects of distributed denial-of-service attacks on MPLS networks

*Béla Genge**, Christos Siaterlis*

Institute for the Protection and Security of the Citizen, Joint Research Centre, Via Enrico Fermi 2749, Ispra (Varese) 21027, Italy

ARTICLE INFO

Article history:
Received 31 December 2012
Accepted 10 April 2013
Available online 19 April 2013

Keywords:
Distributed denial-of-service attacks
MPLS networks
Resilience

ABSTRACT

Modern critical infrastructures such as the power grid are frequently targeted by distributed denial-of-service (DDoS) attacks. Unlike traditional information and communications systems, where the effects of DDoS attacks are mostly limited to the cyber realm, disruptive attacks on critical infrastructure assets can result in the loss of vital services such as transportation and health care. This paper evaluates the effect of disruptive DDoS attacks on multiprotocol label switching (MPLS) networks that provide communications services to many large-scale critical infrastructure assets. The experimental results provide insights into architectural configurations that can increase network resilience without the need to incorporate additional hardware and software.

1. Introduction

Over the last few years there has been a considerable increase in the scope and impact of distributed denial-of-service (DDoS) attacks. These attacks flood targeted systems with packets from thousands of different sources, disrupting communications and services and bringing down even well-defended targets. An example is the recent attack on Spamhaus [10], a massive 300 Gbps packet flood that saturated the company's Internet connections and blocked access to its web pages. The attack was rated as possibly the largest DDoS attack in history. It clearly illustrates the effectiveness of DDoS attacks that employ legitimate services such as DNS to achieve their ends.

Unfortunately, modern critical infrastructures such as power grids, oil and gas pipelines, and water supply systems are constantly exposed to DDoS attacks. A November 2010 study conducted by McAfee [1] involving 200 industry executives in 14 countries revealed that more than 80% of critical infrastructure installations faced DDoS attacks that year. Part of the problem is that security and resilience measures are not made compulsory through policy or regulation, and telecommunications operators are often not aware of the severe risks imposed by the lack of security mechanisms. The situation is exacerbated by the fact that security mechanisms are commonly misconfigured [5,15], potentially rendering the entire security posture ineffective.

The research community has proposed several approaches for designing resilient network topologies. Some of these approaches employ network traffic models that limit input traffic flow to ingress routers based on the available bandwidth [9,14]. However, disruptive DDoS attacks take the hardware and software to their limits, resulting in system states that are difficult to analyze using existing approaches.

In an attempt to address these challenges, this paper focuses on an experimental evaluation of the impact of DDoS attacks on communications in multiprotocol label switching (MPLS) networks. Additionally, it analyzes the applicability of existing traffic models to accurately reflect the real status of networks. The paper argues that existing network simulation tools such as ns-2 have severe limitations in the context of DDoS attacks and that experimental approaches can help provide a realistic view of network behavior.

*Corresponding author.
E-mail address: bela.genge@jrc.ec.europa.eu (B. Genge).

1874-5482/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.ijcip.2013.04.001

The experimental study presented in this paper focused on an isolated environment [6,16] that reproduced a realistic network, including carrier-grade Cisco routers, networks, computer systems, protocols and software. Six MPLS network topologies were created and analyzed with regard to the impact of DDoS attacks on MPLS network traffic as well as the functioning of a simulated remotely controlled power grid. The experiments demonstrate that MPLS virtual private networks (VPNs) alone do not provide proper isolation of virtual circuits, enabling DDoS attacks to severely degrade parallel virtual circuits. The experimental results also show that small changes in network topology can significantly enhance resilience without affecting quality of service (QoS) even when using default router configurations.

2. Problem statement

Modern critical infrastructures such as power grids, oil and gas pipelines, and water supply systems rely on information and communications technologies for their operation. The advantages of using information and communications technologies include reduced costs as well as greater efficiency, flexibility and interoperability. In the past, critical infrastructure assets were largely isolated and used proprietary hardware and protocols, limiting the threats that could affect them. However, the widespread adoption of commercial-off-the-shelf hardware, software and networking products in modern critical infrastructure assets exposes them to disruptive cyber threats.

A DDoS attack on an industrial control system typically engages thousands of infected hosts to flood the victim system with a massive number of packets, consuming network resources and severely reducing communications bandwidth. The result is that the victim system effectively loses its ability to control critical infrastructure assets.

A DDoS attack could ultimately have the same effect as the power grid failure that occurred in Rome on January 2, 2004 [3]. The incident occurred when communications between several remote sites were disabled by a broken water pipe that flooded the server room at a telecommunications service provider, short-circuiting critical hardware. This completely blinded power grid operators, who were unable to monitor and control the remote sites. Fortunately, no additional disturbances occurred during the failure, so the grid remained stable. However, a change in the generated-consumed power balance, possibly caused by weather changes, could have impacted the electrical grid, resulting in a large blackout of the city and affecting other critical infrastructures such as transportation and health care.

Clearly, better protective mechanisms are needed to deal with DDoS attacks, especially in the critical infrastructure, where even short-term outages can have serious consequences. However, there is limited understanding of the effects that DDoS attacks have on real networks, and existing network models and simulation tools are not robust enough to help improve this understanding. For example, existing models [9,14] often incorporate an abstraction layer that does not account for installation-specific aspects. The basic approach taken by such models is to distribute input traffic on output interfaces by employing a variety of algorithms. But in reality, there are many other factors that influence the distribution of packets, especially in the context of DDoS attacks. For instance, a heavily loaded router and network might behave very differently from their predicted behavior. Extreme conditions can lead to loss of input and output packets, rendering simplistic input/output traffic counting techniques inapplicable.

In general, there is a lack of models and simulation tools that can accurately reproduce the network state in extreme conditions such as DDoS attacks. The experiments described in this paper reveal that DDoS attacks have serious consequences on remotely operated critical infrastructure assets even when telecommunications service providers use virtual private networks (VPNs) to isolate traffic. Also, simple topology changes can have a significant impact on network resilience. These changes, which can be deployed using existing routing hardware and software, can help render DDoS attacks ineffective.

3. Experimental study

Our experiments were designed to explore the consequences of information and communications system disruptions on a simulated power grid. In particular, we considered DDoS attacks on telecommunication services that propagate to and impact the power grid. The focus was on evaluating the effectiveness of existing network models and to demonstrate the impact of small network topology changes on the outcome of DDoS attacks.

3.1. *Experimental approach*

The study of complex systems such as modern critical infrastructure assets can be conducted by experimenting with real systems, software simulators or emulators. Unfortunately, for reasons of cost and reproducibility of results, it is difficult to experiment with real systems. Furthermore, if a study seeks to examine the resilience or security of a real system, there are obvious concerns about the potential side effects (faults and disruptions) to mission-critical services.

Software-based simulations can be used very efficiently to study physical systems, primarily because they support low cost, fast and accurate analyses in controlled environments. However, they have limited applicability in the context of cyber security due to the complexity and diversity of real-world networks. Moreover, even when software simulations are able to model network environments, they fail to model network failures with reasonable accuracy [4].

The study described in this paper employed an emulation framework developed in our previous work [6,16], a modern scientific instrument that helps provide accurate assessments of the impact of cyber attacks on cyber-physical systems used in the critical infrastructure. The emulation testbed, which is based on Emulab [16,18], provides fidelity, repeatability, measurement accuracy and safety for the cyber layer. The approach is well-established in the field of cyber security [12], and it helps overcome the challenges that arise while attempting to simulate the behavior of information and communications technology components in the presence of attacks or failures.