Chapter XXXI
Denial-of-Service (DoS) Attacks: Prevention, Intrusion Detection, and Mitigation

Georg Disterer
University of Applied Sciences and Arts, Germany

Ame Alles
University of Applied Sciences and Arts, Germany

Axel Hervatin
University of Applied Sciences and Arts, Germany

ABSTRACT

Since denial-of-service (DoS) attacks are a major threat to e-commerce, waves of DoS attacks against prominent Web pages gained wide publicity. Typically DoS attacks target Web sites with bogus requests for data in order to slow or block legitimate users from accessing services. In recent years, distributed denial-of-service (DDoS) attacks have been used, which expand the vulnerability of Web sites. Attackers use hundreds or thousands of compromised systems in order to harm commercial Web sites. Attackers use different ways to harm their victims. They manipulate the target networks or target server servers directly by using lacks of protocols and standards to force failures and shut-downs. Or, they try to deplete resources like bandwidth, memory, or processing capacities. Attackers try to hinder or interfere with legitimate users with both strategies. Damages from DDoS attacks can range from inconvenience for legitimate users and customers to a lack of reliability for the site and—finally—to a shutdown of the server and some delay until web services are continued. This is a severe threat for all companies involved in e-commerce, and managing that risk is important to offer secure and reliable services. Therefore, management must take actions of prevention, detection and mitigation in order to protect their Web services.

INTRODUCTION

Denial-of-service (DoS) attacks are a major threat to electronic commerce (e-commerce). In 2000 and 2004, waves of DoS attacks against prominent web pages like Yahoo, Google, Double-click, Alta Vista, and others gained publicity. While early attacks on computer networks in the 1980s and 1990s were imputed to

experts with a high level of technical expertise, today nearly anyone can use tools and scripts available on the Internet to attack Web sites. Attackers are no longer experts with high technical or ideological ambitions only, but also script kids using available tools and techniques just for fun or by order of criminals, who try to blackmail companies and threaten them with DoS attacks.

In recent years distributed denial-of-service (DDoS) attacks are used, which expand the vulnerability of Web sites. Attackers use hundreds or thousands of compromised systems in order to harm commercial Web sites. In an empirical study by Ernst & Young (Ernst & Young, 2004) 23% of the respondents indicated that DDoS attacks resulted in an unexpected outage of critical systems in 2003. Scotland Yard got some evidence about trends towards the monetization of Internet crime in the way that criminals offer activities like these under the slogan "rent a botnet" (Reuters, 2004).

Attackers use different ways to harm their victims. They manipulate the target networks or target servers directly by using a lack of protocols and standards to force failures and shutdowns. Or they try to deplete resources like bandwidth, memory, or processing capacities. With both strategies, attackers try to hinder or interfere with legitimate users of the Web site. Damages from DoS and DDoS attacks against a Web site can range from inconvenience for legitimate users and customers, to a lack of reliability of the site and finally to a shutdown of the server and some delay until Web services are continued. This is a severe threat for all companies involved in e-commerce, managing that risk is important to offering secure and reliable services. Therefore, management must take action to prevent, detect, and mitigate, in order to protect Web services. This chapter gives an overview of the risks and threats and a classification of possible countermeasures.

The outage of Web services is a particular threat to companies that rely strongly on the Web to generate revenue, like Internet service providers, online payment services, news providers, online stock brokers, online betting services, and so forth. In addition, attacks damage the image of the effected companies; surveys show a decline in stock price between 1 and 4% shortly after ad hoc disclosures about DoS attacks have been published (Garg, Curtis, & Halper, 2003). In general, these attacks are considered to be one of the most dangerous threats to e-commerce.

CHARACTERISTICS OF DoS AND DDoS ATTACKS

In e-commerce, customers use the Internet to request information about products and services or to settle business transactions. Such requests are usually made by legitimate users who have honest intentions. As providers are interested in fulfilling requests quickly and reliably, the availability of servers is mission critical.

DoS and DDoS attacks try to address this dependency. Typically the attacks are targeted against servers with bogus requests for data in order to slow or block legitimate users from accessing services. Some other types of attacks try to manipulate servers directly in order to cause system outages. With improved security systems, the latter type of attacks today is classified as controllable. However, attacks that try to take up transaction and processing capacities in a way that legitimate users are hindered remain a severe threat to e-commerce.

In the basic form of DoS attacks, attackers try to interfere directly with target servers. An attack method called "ping-flooding" tries to flood a server by sending a high volume of simple requests. Today this type of attack is rarely successful as the resources of the target usually significantly exceed those of the attacker. Only mailbombing is still considered to be a threat in this regard. Once the storage of a mail server has been exceeded, electronic messages of legitimate users cannot be processed until unsolicited messages have been deleted.

About the year 2000, attackers started bundling the resources of multiple systems coordinated in networks