

# Denial-of-Service Attacks

IA 103 Information Security Overview  
Fall Semester, 2008  
Term Paper # 1  
Carlos Torregrosa

“Prominent among the history of notable incidences of malicious code are the denial-of-service (DoS) attacks conducted by Mafiaboy on Amazon.com, CNN.com, ETrade.com, ebay.com, Yahoo.com, Excite.com, and Dell.com. These software-based attacks lasted approximately four hours, and are reported to have resulted in millions of dollars in lost revenue.” (Whitman & Mattord, 2009)

At first glance, the notion of a DoS attack can be very misleading. Many are unaware that such an attack has even occurred when a website is currently unavailable. Furthermore, they do not know that the repercussions of such an attack are much graver than the simple fact they are unable to currently access a website, but has broadly reaching, particularly financial, impacts. The objective of anyone committing such an attack is to essentially slow down the targeted systems and networks to the point of shutting down any and all outside-access to them.

As mentioned earlier, it is easy to overlook the impact of this sort of threat. Particularly with companies that deal primarily with online purchases and services, a DoS attack can easily rack up loss of profit in the thousands and millions of dollars. It is also very interesting to note that small obscure websites are typically not the target of these sorts of attack, usually due to hacker boredom at the ease of which such a feat would be accomplished, and the desire to garner reputation and prestige for their aliases. After all, what makes for a better headline? Yahoo.com was the victim of a DoS attack or the website with the takeout menu for mom-and-pops diner is inaccessible?

In order to know how big of a risk a threat poses to one’s organization, they have to know the value of the assets that they are trying to protect. A crucial step in this process is to create an Information Assurance Baseline that should take into account all of

technical equipment, intellectual property, employees, and other non-tangible assets such as reputation, trust, intellectual property and ideas, etc. Part of this process entails knowing how much revenue an organization typically acquires on a day-to-day basis, which needs to be established through averages over an extended period of time. Using this, we can estimate the expected revenue over a period of time. Through that, we are able to reasonably determine how much money would be lost based on the length of time the DoS attack is in effect and the subsequent time to restore the organization's networks, servers, and all-around functionality. (Boyce & Jennings, 2002)

Before continuing, it is important to note that DoS may not always be the direct result of some sort of malicious activity. If there is some sort of environmental disaster that damages an organizations servers in some fashion, the result can be that of a DoS, without a malicious component. However, it is just as important to note that a DoS attack may just be one component of a much larger and more damaging intrusion. However, it is not something to be taken lightly; and the ease with which one of these attacks can be perpetrated is also of grave concern. (CERT, 1997)

“Some denial-of-service attacks can be executed with limited resources against a large, sophisticated site. This type of attack is sometimes called an "asymmetric attack." For example, an attacker with an old PC and a slow modem may be able to disable much faster and more sophisticated machines or networks. “(CERT, 1997)

While there are defenses, procedures, and controls that can be put in place to help mitigate the risk of a DoS attack it is also impossible to entirely mitigate the risk. While this would hold true for most threats out there, it is particularly noteworthy due to the presence of distributed denial-of-service (DDoS) attacks. In this instance, a large number

of computers, anywhere from several to thousands, launch a coordinated attack to compromise a system. This is often accomplished through the use of zombie computers. Zombie computers are computers that have been taken over in some fashion so that a single entity can command and make use of them remotely to accomplish, in this instance, a DDoS attack. This also makes tracking where the attack actually originated from, nearly impossible. “DDoS attacks are the most difficult to defend against, and there are presently no controls that any single organization can apply. There are, however, some cooperative efforts to enable DDoS defenses among groups of service providers...DDoS is considered a weapon of mass destruction on the Internet.” (Whitman & Mattord, 2009)

DDoS attacks have a number of uses and applications for hackers and even organizations who turn to unethical behaviors. “Internet cafes have grown significantly in the past decade in China... with the rapid growth, competition has also heated up. Due to the ease of launching DDoS attacks, the effectiveness the attacks often achieve, and the difficulty to catch the attacker, some competitors resort to DDoS attacks ... to severely slow down or completely shut down competing Internet cafes. DDoS attacks on Internet cafes have been on the rise both in frequency and in magnitude. However, due to the relatively small scale and low profit margin of most Internet cafes, it is difficult for individual Internet cafes to afford effective means to defend against DDoS attacks on their own. Although low-end, PC based software DDoS solutions are available, they easily fail under heavy attacks.” (IntruGuard Devices)

A DoS attack can be implemented or take effect through a number of different weaknesses and/or vulnerabilities in a system. Firstly, a system cannot have unlimited

resources available to it in terms of “network bandwidth, memory and disk space, CPU time, data structures, access to other computers and networks, and certain environmental resources...” That makes those items very large targets for hackers to target in order to bring about DoS for the organization. While each may require different steps and processes to accomplish using up or controlling the resource, the end-result is the same, if the system no longer has access to what it requires to function, it will be unable to do so. Another way for a DoS attack to be implemented is by having critical configuration information either of a computer, network, router, server, etc., being altered or destroyed in some fashion, essentially cutting off access. (CERT, 1997)

What can be done to protect or recover from a DoS attack? One of the first steps to take is to ensure the physical security and access to critical components of your organization’s servers and networks. Based on a cost-to-benefit analysis that will need to be calculated for an individual organization, technical controls can be put into place. Alongside that, policy, procedures, and guidelines need to be established to promote awareness within an organization at all levels. It is widely believed and spoken that people are the weakest link in any organization’s security. Make sure that technical equipment is properly maintained and updated with the latest patches. Create an Incident Recovery plan, Disaster Recovery plan, and other documentation to cover a DoS scenario. This will provide an organization with carefully thought out plans to be able to recover from a successful attack as swiftly as possible. (Boyce & Jennings, 2002)

## **Bibliography**

Boyce, J.G., & Jennings, D.W. (2002). *Information assurance Managing organizational IT security risks*. USA: Butterworth-Heinemann.

Carnegie Mellon University., (1997, October 2nd). Denial of service attacks. Retrieved October 13, 2008, from CERT Web site:  
[http://www.cert.org/tech\\_tips/denial\\_of\\_service.html](http://www.cert.org/tech_tips/denial_of_service.html)

Case Study Protecting Internet Cafes from DoS/DDoS. Retrieved October 14, 2008, from IntruGuard Devices Web site:  
<http://www.intruguard.com/documents/MSSPInternetCafeCaseStudy.pdf>

Whitman, M.E., & Mattord, H.J. (2009). *Principles of information security Third edition*. Canada: Thompson Course Technology.