Information Security and Ethics:

Concepts, Methodologies, Tools, and Applications

Hamid Nemati
The University of North Carolina at Greensboro, USA

Information Science REFERENCE

INFORMATION SCIENCE REFERENCE
Hershey · New York

Assistant Executive Editor:	Meg Stocking
Acquisitions Editor:	Kristin Klinger
Development Editor:	Kristin Roth
Senior Managing Editor:	Jennifer Neidig
Managing Editor:	Sara Reed
Typesetter:	Amanda Appicello
Cover Design:	Lisa Tosheff
Printed at:	Yurchak Printing Inc.

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue, Suite 200
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-pub.com
Web site: http://www.igi-pub.com/reference

and in the United Kingdom by
Information Science Reference (an imprint of IGI Global)
3 Henrietta Street
Covent Garden
London WC2E 8LU
Tel: 44 20 7240 0856
Fax: 44 20 7379 0609
Web site: http://www.eurospanonline.com

Library of Congress Cataloging-in-Publication Data

Knowledge management : concepts, methodologies, tools and applications / Murray Jennex, editor.
p. cm.
Summary: "This is the defining reference source for all theories, concepts, and methodologies within the KM discipline. It includes chapters on Implementing KM in Organizations; KM Systems Acceptance; KM Communication; Knowledge Representation; Knowledge Sharing; KM Success Models; Knowledge Ontology; and Operational KM, and provides libraries with the defining reference to the field"--Provided by publisher.
Includes bibliographical references and index.
ISBN-13: 978-1-59904-933-5 (hardcover)
ISBN-13: 978-1-59904-934-2 (ebook)
1. Knowledge management. I. Jennex, Murray E., 1956-
HD30.2.K636866 2008
658.4'038--dc22
2007027566

Copyright © 2008 by IGI Global. All rights reserved. No part of this publication may be reproduced, stored or distributed in any form or by any means, electronic or mechanical, including photocopying, without written permission from the publisher.

Product or company names used in this set are for identification purposes only. Inclusion of the names of the products or companies does not indicate a claim of ownership by IGI Global of the trademark or registered trademark.

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 1.1
E-Government and Denial of Service Attacks

Aikaterini Mitrokotsa
University of Piraeus, Greece

Christos Douligeris
University of Piraeus, Greece

ABSTRACT

The use of electronic technologies in government services has played a significant role in making citizens' lives more convenient. Even though the transition to digital governance has great advantages for the quality of government services it may be accompanied with many security threats. One of the major threats and hardest security problems e-government faces are the denial of service (DoS) attacks. DoS attacks have already taken some of the most popular e-government sites off-line for several hours causing enormous losses and repair costs. In this chapter, important incidents of DoS attacks and results from surveys that indicate the seriousness of the problem are presented. In order to limit the problem of DoS attacks in government organizations, we also present a list of best practices that can be used to combat the problem together with a classification of attacks and defense mechanisms.

INTRODUCTION

Since we live in a world where electronic and Internet technologies are playing an important role in helping us lead easier lives, local and state governments are required to adopt and participate in this technology revolution. Digital government or e-government technologies and procedures allow local and national governments to disseminate information and provide services to their citizens and organisations in an efficient and convenient way resulting in reducing waiting lines in offices and in minimizing the time to pick up and return forms and process and acquire information. This modernization of government facilitates the connection and cross cooperation of authorities in several levels of government—central, regional, and local—allowing an easy interchange of data and access to databases and resources that would be impossible otherwise.

Copyright © 2008, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

E-government undoubtedly makes citizens' lives and communication easier by saving time, by avoiding and bypassing the bureaucracy, and by cutting down paper work. It also provides the same opportunities for communication with government not only to people in cities but also to people in rural areas. Moreover, e-government permits greater access to information, improves public services, and promotes democratic processes.

This shift to technology use and the transition to a "paperless government" is constantly increasing. According to Holden, Norris, and Fletcher (2003), in 1995 8.7% of local governments had Web sites, while in 2003 this number showed an increase that reached 83%. Despite these encouraging statistics, the adoption of digital government proceeds with a slow pace as security issues, like confidentiality and reliability, affect the fast progress of e-government. Since e-government is mainly based on Internet technologies, it faces the danger of interconnectivity and the well-documented vulnerabilities of the Internet infrastructure. The Institute for E-Government Competence Center (IFG.CC, 2002) states that in 2002, 36 government Web sites were victims of intrusions. Most of the e-government attacks have taken place in Asia (25%) and more precisely in China and Singapore (19%), as well as in the USA (19%).

According to the U.S. Subcommittee on Oversight and Investigations (2001), the FedCIRC incident records indicate that in 1998 the number of incidents that were reported was 376, affecting 2,732 U.S. Government systems. In 1999, there were 580 incidents causing damage on 1,306,271 U.S. Government systems and in 2000 there were 586 incidents having impact on 575,568 U.S. government systems. Symantec (2004) (Volume VI, released September 2004, activity between January 2004 and June 2004) gives information about Government specific attack data. In this report, one can see that the third most common attack e-government has faced, besides worm-related attacks and the Slammer worm, is the TCP SYN Flood denial of service attack.

So in order to have effective e-government services without interruptions in Web access as well as e-mail and database services, there is a need for protection against DoS attacks. Only with reliable e-government services not threatened by DoS attacks governments may gain the trust and confidence of citizens.

Moore, Voelker, and Savage (2001) state that the denial of service (DoS) attacks constitute one of the greatest threats in globally connected networks, whose impact has been well demonstrated in the computer network literature and have recently plagued not only government agencies but also well known online companies. The main aim of DoS is the disruption of services by attempting to limit access to a machine or service. This results in a network incapable of providing normal service either because its bandwidth or its connectivity has been compromised. These attacks achieve their goal by sending at a victim a stream of packets in such a high rate so that the network is rendered unable to provide services to its regular clients.

Distributed denial of service (DDoS) is a relatively simple, yet very powerful, technique to attack Internet resources. DDoS attacks add the many-to-one dimension to the DoS problem making the prevention and mitigation of such attacks more difficult and their impact proportionally severe.

DDoS attacks are comprised of packet streams from disparate sources. These attacks use many Internet hosts in order to exhaust the resources of the target and cause denial of service to legitimate clients. DoS or DDoS attacks exploit the advantage of varying packet fields in order to avoid being traced back and characterized. The traffic is usually so aggregated that it is difficult to distinguish between legitimate packets and attack packets. More importantly, the attack volume is often larger than the system can handle. Unless special care is taken, a DDoS victim can suffer damages ranging from system shutdown and file corruption to total or partial loss of services.

Extremely sophisticated, “user-friendly,” and powerful DDoS toolkits are available to potential attackers increasing the danger that an e-government site becomes a victim in a DoS or a DDoS attack by someone without a detailed knowledge of software and Internet technologies. Most of the DDoS attack tools are very simple and have a small memory size something that is exploited by attackers, who achieve easily implementation and manage to carefully hide the code. Attackers constantly modify their tools to bypass security systems developed by system managers and researchers, who are in a constant alert to modify their approaches in order to combat new attacks.

The attackers in order to have more devastating results change their tactics and the way they launch DoS attacks. One of these tactics is the silent degradation of services for a long period of time in order to exhaust a large amount of bandwidth instead of a quick disruption of network services.

The result of these attacks in government organisations among others include reduced or unavailable network connectivity and, consequently, reduction of the organisation’s ability to conduct legitimate business on the network for an extended period of time. The duration and the impact of the attack depends on the number of possible attack networks. It is also worth bearing in mind that even if an organisation is not the target of an attack, it may experience increased network latency and packet losses, or possibly a complete outage, as it may be used from the attacker in order to launch a DDoS attack.

In this chapter, we stress the severity that a DoS attack may have for e-government agencies. To this end, statistics and characteristic incidents of DoS attacks in e-government agencies are presented. Furthermore, we present a classification of DoS and DDoS attacks, so that one can have a good view of the potential problems. Moreover, we outline a list of best practices that can be used in government organisations in order to further strengthen the security of their systems and to help them protect their systems from being a part of a distributed attack or being a target of DoS/DDoS attacks. Long-term countermeasures are also proposed that should be adopted for more efficient solutions to the problem.

Following this introduction, this chapter is organised as follows. In the section “Denial of Service Attacks” the problem of DoS attacks is investigated, DoS incidents and results from surveys related to DoS attacks, and a classification of DoS attacks are presented. In the section “Distributed Denial of Service Attacks” the problem of DDoS attacks is introduced, giving the basic characteristics of well known DDoS tools, and presenting a taxonomy of DDoS attacks. In the section “Classification of DDoS Defense Mechanisms,” we present the DDoS defense problems and propose a classification of DDoS defense mechanisms. In the section “Best Practices for Defeating Denial of Service Attacks” best practices for defeating DoS attacks that can be used by government organizations are presented, while in the section “Long Term Countermeasures” some long-term efforts against DoS attacks are presented.

DENIAL OF SERVICE ATTACKS

Defining Denial of Service Attacks

The WWW Security FAQ (Stein & Stewart, 2002) states that “a DoS attack can be described as an attack designed to render a computer or network incapable of providing normal services.” In a DoS attack, a computer or network resource is blocked or degraded resulting in unavailable system resources but not necessarily in the damage of data.

The most common DoS attacks target the computer network’s bandwidth or connectivity (Stein & Stewart, 2002). In bandwidth attacks, the network is flooded with a high volume of traffic leading to the exhaustion of all available network resources, so that legitimate user requests cannot get through, resulting in degraded productivity. In connectivity attacks, a computer is flooded with a high volume of connection requests leading to the exhaustion of all available operating system resources, thus rendering the computer unable to process legitimate user requests.

Denial of Service Incidents

Undoubtedly, DoS attacks are a threatening problem for the Internet, causing disastrous financial losses by rendering organisations' sites off-line for a significant amount of time as we can easily confirm by frequent news reports naming as victims of DoS attacks well-known large organisations with significant exposure in the e-economy.

Howard (1998) reports denial of service attacks' statistics where one can see the dramatic increase in such attacks even in the first years of the Web. The Internet Worm (Spafford, 1998) was a prominent story in the news because it "DoS-ed" hundreds of machines. But it was in 1999 when a completely new breed of DoS attacks appeared. The so-called distributed denial of service attacks stroke a huge number of prominent Web sites.

Criscuolo (2000) reports that the first DDoS attack occurred at the University of Minnesota in August 1999. The attack, flooding the Relay chat server, lasted for two days and it was estimated that at least 214 systems were involved in the attack launch. In February 2000, a series of massive denial-of-service (DoS) attacks rendered out of service several Internet e-commerce sites including Yahoo.com. This attack kept Yahoo off the Internet for 2 hours and lead Yahoo a significant advertising loss. In October 2002 (Fox News, 2002), 13 routers that provide the DNS service to Internet users were victims of a DDoS attack. Although the attack lasted only for an hour, 7 of the 13 root servers were shut down, something that indicates the potential vulnerability of the Internet to DDoS attacks. In January of 2001, Microsoft's (WindowsITPro, 2001) Web sites hosting Hotmail, MSN, Expedia, and other major services were inaccessible for about 22 hours because of a DDoS attack. Despite attacks on high-profile sites, the majority of the attacks are not well publicized for obvious reasons.

CERT (2001) reports that in July 2001, the Whitehouse Web site was the target of the Code Red worm. The attack on the Whitehouse lasted from about 8 a.m. to about 11:15 a.m. Between 1 p.m. and 2 p.m., page request continued failing, while after 2 p.m. the site was occasionally inaccessible. In order to alleviate the effects of the attack, the Whitehouse momentarily changed the IP address of the Whitehouse.gov Web site.

Sophos.com (2002) reports that in June 2002, the Pakistani's Government Web site accepted a DoS attack that was launched by Indian sympathizers. The attack was launched through a widespread Internet worm called W32/Yaha-E, which encouraged Indian hackers and virus writers to launch an attack against Pakistan Government sites. The worm arrived as an e-mail attachment and its subject was relative to love and friendship. The worm highlighted the political tensions between Indian and Pakistan and managed to render the www.pak.gov.pk Web site unreachable. The worm created a file on infected computers that urged others to participate in the attack against the Pakistani government.

ITworld.com (2001) reports that even the site of CERT was the victim of a DDoS attack on May 28, 2001. Although the CERT Coordination Center is the first place where someone can find valuable information in order to be prevented against malicious cyber attacks it was knocked offline for two days by a DDoS attack accepting information at rates several hundred times higher than normal.

Cs3.Inc (2005) reports that a DDoS attack was launched on the U.S. Pacific command in April 2001. The source addresses of the attack belonged to the People's Republic of China, although the exact origin of the attack has yet not been identified. Despite the fact that the internal networks of the command were not affected, in the long-term no one can deny the fact that critical government operations may be easily disrupted by attackers. After this incident, the political tension between the two countries increased considerably. The U.S. government worries that U.S. critical network assets may be a target of a DDoS attack as a digital continuation of the terrorist attacks against New York in September of 2001. But government systems can not only be victims of DoS attacks, but may also be used unwittingly in order for a DoS attack to be performed by hosting the agents of a DDoS attack, thus participating involuntarily in the conduction of the attack.

Moore et al. (2001) report that in February of 2001, UCSD network researchers from the San Diego Supercomputer Center (SDSC) and the Jacobs School of Engineering analyzed the worldwide pattern of malicious denial-of-service (DoS) attacks against the computers of corporations, universities, and private individuals. They proposed a new technique, called "backscatter analysis" that gives an estimate of worldwide denial of service activity. This research provided the only publicly available data quantifying denial of service activity in the Internet and enabled network engineers to understand the nature of DoS attacks.

The researchers used data sets that were collected and analyzed in a three-week long period. They assessed the number, duration, and focus of the attacks, in order to characterize their behaviour and observed that more than 12,000 attacks against more than 5,000 distinct targets, ranging from well-known e-commerce companies to small foreign Internet service providers and even individual personal computers on dial-up connections. Some of the attacks flooded their targets with more than 600,000 messages/packets per second.

In addition, they reported that 50% of the attacks were less than ten minutes in duration, 80% were less than thirty minutes, and 90% lasted less than an hour. Two percent of the attacks were longer than five hours, 1% is greater than ten hours, and a few dozen spanned multiple days. Furthermore, according to this research, 90% were TCP-based attacks and around 40% reached rates as high as 500 packets per second (pps) or greater. Analyzed attacks peaked at around 500,000 pps, while other anecdotal sources report larger attacks consuming 35 megabits per second (Mbps) for periods of around 72 hours, with high-volume attacks reaching 800 Mbps.

The Computer Security Institute (2003) in the 2003 CSI/FBI survey reported that denial of service attacks represent more than a third among the WWW site incidents, where unauthorized access or misuse was conducted. Forty-two percent of respondents to the 2003 survey reported DoS attacks. In 2000, 27% reported such attacks. There appears to be a significant upward trend in DoS attacks. The Computer Security Institute (2004) in the 2004 CSI/FBI survey reported that the highest reported financial losses due to a single DoS attack increased from $1 million in 1998 to $26 million in 2004 and emerged for the first time as the incident type generating the largest total losses.

We should also keep in mind that many government organisations interpret DDoS attacks as simply being an experience of inadequate service from their ISP and are not aware that they are under attack. This has as result the fact that nine out of ten DDoS attacks go unreported. In spite of such evidence, most government organisations overlook the necessity of using preventive mechanisms to combat DoS attacks.

Although there is no panacea for all types of DoS attacks, there are many defense mechanisms that can be used in order to make the launch of an attack more difficult and provide the means to reach the disclosure of the identity of the attacker.

Denial of Service Attack Classification

DoS attacks can be classified into five categories based on the attacked protocol level. More specifically, Karig and Lee (2001) divide DoS attacks in attacks in the *Network Device Level*, the *OS Level*, *application based attacks*, *data flooding attacks*, and *attacks based on protocol features.*

DoS attacks in the Network Device Level include attacks that might be caused either by taking advantage of bugs or weaknesses in software, or by exhausting the hardware resources of network devices. One example of a network device exploit is the one that is caused by a buffer-overrun error in the password checking routine. Using this exploit, certain routers (Karig et al., 2001) could be crashed if the connection to the router is performed via telnet and entering extremely long passwords.

The OS level DoS attacks (Karig et al., 2001) take advantage of the ways protocols are implemented by operating systems. One example of this category of DoS attacks is the Ping of Death attack (Insecure.org, 1997). In this attack, ICMP echo requests having data sizes greater than the maximum IP standard size are sent to the victim. This attack often results in the crashing the victim's machine.

Application-based attacks try to take a machine or a service out of order either by exploiting bugs in network applications that are running on the target host or by using such applications to drain the resources of their victim. It is also possible that the attacker may have found points of high algorithmic complexity and exploits them in order to consume all available resources on a remote host. One example of an application-based attack (Karig et al., 2001) is the finger bomb. A malicious user could cause the finger routine to be recursively executed on the victim, in order to drain its resources.

In *data flooding attacks*, an attacker attempts to use the bandwidth available to a network, host, or device at its greatest extent, by sending massive quantities of data and so causing it to process extremely large amounts of data. An example is flood pinging.

DoS attacks *based on protocol features* take advantage of certain standard protocol features. For example, several attacks exploit the fact that IP source addresses can be spoofed. Moreover, several types of DoS attacks attempt to attack DNS cache on name servers. A simple example of attacks exploiting DNS is when an attacker owning a name server traps a victim name server into caching false records by querying the victim about the attacker's own site. If the victim name server is vulnerable, it would then refer to the malicious server and cache the answer.

DISTRIBUTED DENIAL OF SERVICE ATTACKS

Defining Distributed Denial of Service Attacks

The WWW Security FAQ (Stein & Stewart, 2002) states "A DDoS attack uses many computers to launch a coordinated DoS attack against one or more targets. Using client/server technology, the perpetrator is able to multiply the effectiveness of the DoS significantly by harnessing the resources of multiple unwitting accomplice computers, which serve as attack platforms." It is distinguished from other attacks by its ability to deploy its weapons in a "distributed" way over the Internet and to aggregate these forces to create lethal traffic. The main goal of a DDoS attack is to cause damage on a victim either for personal reasons or for material gain or for popularity.

Mirkovic, Martin, and Reiher (2001) state that the following Internet characteristics make DDoS attacks very destructive:

1. **Interdependency of Internet security:** When a machine is connected to the Internet, it is also connected to countless insecure and vulnerable hosts, making it difficult to provide a sufficient level of security.
2. **Limited resources:** Every host in the Internet has unlimited resources, so sooner or later its resources will be consumed.
3. **Many against afew:** If the attacker's resources are greater than the victim's resources then a DDoS attack is almost inevitable.

DDoS Strategy

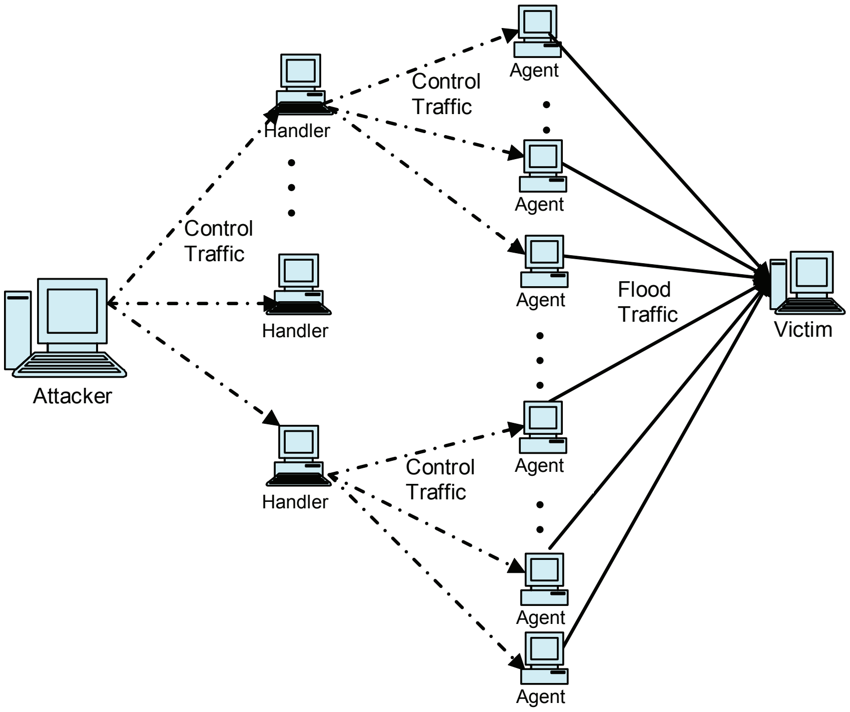
A distributed denial of service attack is composed of four elements, as shown in Figure 1.

1. The *real attacker*
2. The *handlers or masters*, who are compromised hosts with a special program capable of controlling multiple agents, running on them (Cisco Systems, Inc., 2006)
3. The attack daemon agents or zombie hosts, who are compromised hosts, running a special program and generate a stream of packets towards the victim (Cisco Systems, Inc., 2006)
4. A *victim* or *target host*

The following steps take place in order to prepare and conduct a DDoS attack:

- **Step 1. Selection of agents:** The attacker chooses the agents that will perform the attack. The selection of the agents is based on the existence of vulnerabilities in those machines that can be exploited by the attacker in order to gain access to them.
- **Step 2. Compromise:** The attacker exploits the security holes and vulnerabilities of the agent machines and plants the attack code.

Figure 1. Architecture of DDoS attacks



Furthermore, the attacker tries to protect the code from discovery and deactivation. Self-propagating tools such as the Ramen worm (CIAC Information Bulletin, 2001) and Code Red (CERT, 2001) soon automated this phase. When participating in a DDoS attack, each agent program uses only a small amount of resources (both in memory and bandwidth), so that the users of computers experience minimal change in performance The people who use the agent systems do not know that their systems are compromised and used for the launch of a DDoS attack (Specht & Lee, 2003). When participating in a DDoS attack, agent programs consume little resources this means that the users of computers experience minimal change in performance.

- **Step 3. Communication** (Specht et al., 2003)**:** Before the attacker commands the onset of the attack, he communicates with the handlers in order to find out which agents can be used in the attack, if it is necessary to upgrade the agents and when is the best time to schedule the attack.
- **Step 4. Attack:** At this step, the attacker commands the onset of the attack (Mirkovic, 2002). The victim and the duration of the attack as well as special features of the attack such as the type, port numbers, length, TTL, and so forth can be adjusted.

In a new generation of DDoS attacks, the onset of the attack is not commanded by the attacker but starts automatically during a monitoring procedure of a public location on the Internet. For instance, a chat room may be monitored and when a specific word is typed the DDoS attack is triggered. It is even more difficult to trace the attacker and reveal its true origin in such an environment. We can understand the enormity of the danger if the trigger word or phrase is commonly used.

Specht et al. (2003) state that a multi-user, online chatting system known as Internetrelay chat (IRC) channels is often used for the communication between the attacker and the agents, since IRC chat networks allow their users to create public, private and secret channels. An IRC-based DDoS attack model does not have many differences computed to the agent-handler DDoS attack model except from the fact that an IRC server is responsible for tracking the addresses of agents and handlers and for facilitating the communication between them. The main advantage of the IRC-based attack model over the agent-handler attack model is the anonymity it offers to the participant of the attack.

DDoS Tools

There are several known DDoS attack tools. The architecture of these tools is very similar whereas some tools have been constructed through minor modifications of other tools. In this section, we present the functionality of some of these tools. For presentation purposes, we divide them in *agent-based* and *IRC-based* DDoS tools.

Agent-based DDoS tools are based on the agent—handler DDoS attack model that consists of handlers, agents, and victim(s) as it has already been described in the section on DDoS attacks. Some of the most known agent-based DDoS tools are the following: *Trinoo, TFN, TFN2K, Stacheldraht, mstream, and Shaft*.

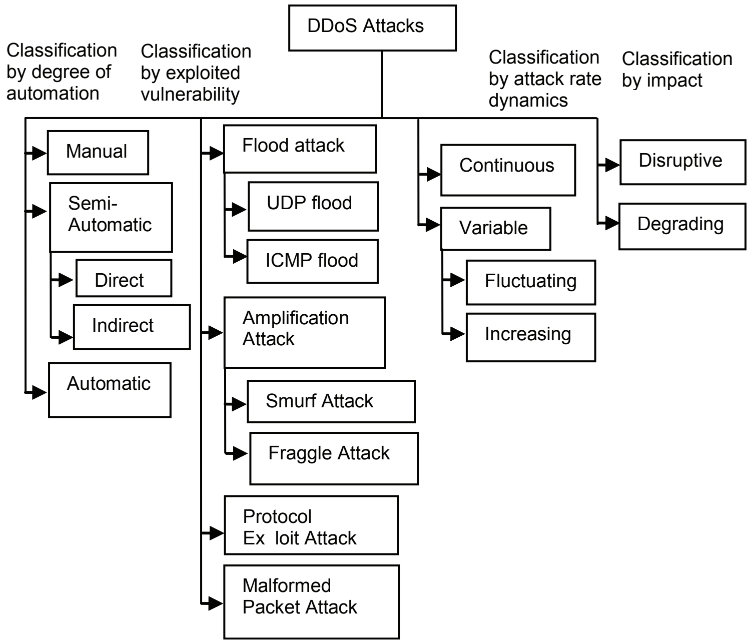
Trinoo (Criscuolo, 2000) is the most known and mostly used DDoS attack tool. It is a tool that is able to achieve bandwidth depletion and can be used to launch UDP flood attacks. *Tribe Flood Network (TFN)* (Dittrich, 1999a) is a DDoS attack tool that is able to perform resource and bandwidth depletion attacks. Some of the attacks that can be launched by TFN include Smurf, UDP flood, TCP SYN flood, ICMP echo request flood, and ICMP directed broadcast. *TFN2K* (Barlow & Thrower, 2000) is a derivative of the TFN tool and is able to implement Smurf, SYN, UDP, and ICMP Flood attacks. TFN2K has a special feature of being able to add encrypted messaging between all of the attack components (Specht et al., 2003). *Stacheldraht* (Dittrich, 1999b) (German term for "barbed wire"), that is based on early versions of TFN, attempts to eliminate some of its weak points and implement Smurf, SYN Flood, UDP Flood, and ICMP Flood attacks. *Mstream* (Dittrich, Weaver, Dietrich, & Long, 2000) is a simple TCP ACK flooding tool that is able to overwhelm the tables used by fast routing routines in some switches. *Shaft* (Dietrich et al., 2000) is a DDoS tool similar to Trinoo that is able to launch packet flooding attacks by controlling the duration of the attack as well as the size of the flooding packets.

Many IRC-based DDoS tools are very sophisticated as they include some important features that are also found in many agent-handler attack tools. One of the most known IRC-based DDoS tools is *Trinity* (Hancock, 2000). *Trinity v3* (Dietrich et al., 2000) besides the up to now well-known UDP, TCP SYN, TCP ACK, TCP NUL packet floods introduces TCP fragment floods, TCP RST packet floods, TCP random flag packet floods, and TCP established floods. In the same generation with Trinity is *myServer* (Dietrich et al., 2000) and *Plague* (Dietrich et al., 2000). MyServer relies on external programs to provide DoS and Plague provides TCP ACK and TCP SYN flooding. *Knight* (Bysin, 2001) is a very lightweight and powerful IRC-based DDoS attack tool able to perform UDP Flood attacks, SYN attacks and an urgent pointer flooder. A DDoS tool that is based on Knight is *Kaiten* (Specht et al., 2003). Kaiten includes UDP, TCP flood attacks, SYN, and PUSH+ACH attacks and it also randomizes the 32 bits of its source address.

DDoS Classification

To be able to understand DDoS attacks it is necessary to have a formal classification. We propose a classification of DDoS attacks that combines efficiently the classifications proposed by Mirkovic et al. (2001), Specht et al. (2003), and

Figure 2. Classification of DDoS attacks



more recent research results. This classification is illustrated in Figure 2 and consists of two levels. In the first level, attacks are classified according to their degree of automation, exploited vulnerability, attack rate dynamics and their impact. In the second level, specific characteristics of each first level category are recognized.

CLASSIFICATION OF DDOS DEFENSE MECHANISMS

DDoS attack detection is extremely difficult. The distributed nature of DDoS attacks makes them extremely difficult to combat or trace back. Moreover, the automated tools that make the deployment of a DDoS attack possible can be easily downloaded. Attackers may also use IP spoofing in order to hide their true identity. This spoofing makes the traceback of DDoS attacks even more difficult.

We may classify DDoS defense mechanisms using two different criteria. The first classification categorizes the DDoS defense mechanisms according to the activity deployed as follows:

1. **Intrusion prevention:** Tries to stop DDoS attacks from being launched in the first place.
2. **Intrusion detection:** Focuses on guarding host computers or networks against being a source of network attack as well as being a victim of DDoS attacks either by recognizing abnormal behaviours or by using a database of known.
3. **Intrusion response:** Tries to identify the attack source and block its traffic accordingly.
4. **Intrusion tolerance and mitigation:** Accepts that it is impossible to prevent or stop DDoS attacks completely and focuses on minimizing the attack impact and on maximizing the quality of the offered services.

The second classification divides the DDoS defenses according to the location deployment resulting (Mirkovic, 2002) into the following three categories of defense mechanisms:

1. **Victim network mechanisms:** Helps the victim recognize when it is the main target of an attack and gain more time to respond.
2. **Intermediate network mechanisms:** Are more effective than victim network mechanisms since they achieve a better handling of the attack traffic and an easier tracing back to the attackers.
3. **Source network mechanisms*:*** Trys to stop attack flows before they enter the Internet core and facilitate the traceback and investigation of an attack.

The previous classification of DDoS defense mechanisms is described thoroughly in Douligeris and Mitrokotsa (2004).

BEST PRACTICES FOR DEFEATING DENIAL OF SERVICE ATTACKS

DoS attacks can lead to a complete standstill of entire government organisations, thereby costing millions of dollars in lost revenue and/or productivity and moving citizens away from e-services. Some governments do not understand the seriousness of the problem, resulting in vulnerable and easy to compromise systems. These systems pose a threat not only to the organisations themselves but also to anyone else targeted by a hacker through these systems. This means it is critical to take preemptive measures to reduce the possibility of these attacks and minimize their impact.

Since DoS attacks are extremely complicated one must note that there is no single-point solution and no system is secure proof. No one can deny though that with effective advance planning government agencies could respond efficiently and rapidly to security threats like denial of service. Below we list some practices that can be used in order to reduce these attacks and diminish their impact.

1. **Establish a security policy and educate:** As stated by Walters (2001), it is of great importance to establish and maintain a security policy. In addition to covering the basics of antivirus, user access, and software updates, on no account one should neglect to address ways to combat DoS/DDoS attacks in such a policy. Moreover, a security policy should be adequately communicated to all employees. It is important to verify that the knowledge skills of system administrators and auditors are current, something that can be achieved by frequent certifications. Of great importance is the continuous training of the organisation's personnel in new technologies and forensic techniques.
2. **Use multiple ISPs:** Government organisations should consider using more than one ISP, in order to make a DoS/DDoS attack against them harder to carry out. In the selection of ISPs, it is important to keep in mind that providers should use different access routes in order to avoid a complete loss of access in the case one pipe becomes disabled (Walters, 2001). It has also been proposed to set legislation to make it obligatory for ISPs to set up egress filtering.
3. **Load balancing:** Specht et al. (2003) state that a good approach in order to avoid being a victim of DoS attacks is to distribute an organisation's systems' load across multiple servers. In order to achieve this, a "Round Robin DNS" or hardware routers could be used to send incoming requests to one or many servers.
4. **Avoid a single point failure:** In order to avoid a single point failure the best solution is to have redundant ("hot spares") machine that can be used in case a similar machine is disabled (Householder, Manion, Pesante, Weaver, & Thomas, 2001). Furthermore, organisations should develop recovery plans that will cover each potential failure point of their system. In addition, organisations should use multiple operating systems in order to create "biodiversity" and avoid DoS attack tools that target specific Operating Systems (OSs).
5. **Protect the systems with a firewall:** Walters (2001) states that since the exposure to potential intruders is increasing, the installation of firewalls that tightly limit transactions across the systems' periphery government organisations should be built to provide effective defenses. Firewalls should be configured appropriately keeping open only the necessary ports. In addition, firewalls are able to carefully control, identify, and handle overrun attempts. Moreover, ingress filtering should be established in government Web servers so that they cannot be used as zombies for launching attacks on other servers. Government departments should also specify a set of IP addresses that could be used only by Government servers.
6. **Disable unused services:** It is important, that as Leng and Whinston (2000) state, organisations' systems remain simple by minimizing the number of services running on them. This can be achieved by shutting down all services that are not required. It is important to turn off or restrict specific services that might otherwise be compromised or subverted in order to launch DoS attacks. For instance, if UDP echo or character generator services are not required, disabling them will help to defend against attacks that exploit these services.
7. **Be up to date on security issues:** As it is widely known the best way to combat DoS attacks is to try to be always protected and up-to-date on security issues (Householder et al., 2001). It is important to be informed

about the current upgrades, updates, security bulletins, and vendor advisories in order to prevent DoS attacks. Thus, the exposure to DoS attacks can be substantially reduced, although one would not expect the risk to be eliminated entirely.

8. **Test and monitor systems carefully:** The first step in order to detect anomalous behaviour is to “characterize” what normal means in the context of a government agency’s network. The next step should be the auditing of access privileges, activities, and applications. Administrators should perform 24x7 monitoring in order to reduce the exhausting results of DoS attacks that inflict government servers. Through this procedure, organisations would be able to detect unusual levels of network traffic or CPU usage (Householder et al., 2001). There are a variety of tools that are able to detect, eliminate, and analyze denial-of-service attacks.
9. **Mitigate spoofing:** An approach that intruders often use in order to conceal their identity when launching DoS attacks is source-address spoofing. Although it is impossible to completely eliminate IP spoofing, it is important to mitigate it (Singer, 2000). There are some approaches that can be used in order to make the origins of attacks harder to hide and to shorten the time to trace an attack back to its origins. System administrators can effectively reduce the risk of IP spoofing by using ingress and egress packet filtering on firewalls and/or routers.
10. **Stop broadcast amplification:** It is important to disable inbound directed broadcasts in order to prevent a network from being used as an amplifier for attacks like ICMP Flood and Smurf (Leng et al., 2000). Turning off the configuration of IP directed broadcast packets in routers and making this a default configuration is the best action that could be performed by network hardware vendors.
11. **DNS for access control should not be used:** Using hostnames in access list instead of IP addresses make systems vulnerable to name spoofing (Leng et al., 2000). Systems should not rely on domain or host names in order to determine if an access is authorized or not. Otherwise, intruders can masquerade a system, by simply modifying the reverse-lookup tables.
12. **Create an incident response plan:** It is important to be prepared and ready for any possible attack scenario. Government organisations should define a set of clear procedures that could be followed in emergency situations and train personnel teams with clearly defined responsibilities ready to respond in emergency cases (Householder et al., 2001). Any attacks or suspicious system flaws should be reported to local law enforcement and proper authorities (such as FBI and CERT) so that the information could be used for the defense of other users as well.

LONG-TERM COUNTERMEASURES

The variety and sophistication of DoS attacks are likely to increase, so despite the defensive measures that can be used now, we need to confront DoS attacks as a problem that requires a long-term effort in order to define and implement effective solutions. It is important to note here that governments should adopt a non-intrusive approach for the protection against DoS attacks while there is a fine line between limiting criminal activity and limiting economy, education, information, and personal freedoms.

Suns Institute (2000) identifies some actions that will help in defending against DoS attacks more effectively in the distant future. Among them one finds the accelerated adoption of the IPsec components of IPv6 and Secure DNS. It is important that the security updating process be automated. Vendors should be encouraged to implement this on behalf of their clients in order to make it easier to update their products and provide information on security issues. Furthermore, research and development of safer operating systems is necessary. Topics to be addressed should include among others anomaly-based detection and other forms of intrusion detection. In addition, governments should consider making some changes in their government procurement policies in a way that security and safety are emphasized.

A significant role in the fight against denial of service attacks would be the establishment of organisations that would be responsible for network security monitoring and incident handling. These organisations should encourage the public awareness about security issues, inform critical owners' infrastructures and government departments about threats, promote and encourage the adoption and production of security standards and maintain statistics and incident databases as well as cooperate with similar organisations (e.g., CERT).

Governments should also ensure that government agencies take all the necessary steps in order to ensure their IT security. Government departments should encourage a better investigation of computer attacks while respecting the privacy and personal rights of Internet users. Additional funding for the training of expert personnel in securing IT Technologies and educating citizens in order to be prevented from cyber crime is a must. It is also important to promote and encourage law enforcement authorities to prosecute perpetrators across national borders and examine the legal framework to facilitate this cooperation.

CONCLUSION

Undoubtedly, DoS attacks should be treated as a serious problem in the Internet. Their rate of growth and wide acceptance challenge the general public's view of electronic transactions and create skeptical governments and businesses. No one can deny that DoS attacks will continue to pose a significant threat to all organisations including government organisations. New defense mechanisms will be followed by the emergence of new DoS attack modes. A network infrastructure must be both robust enough to survive direct DoS attacks and extensible enough to adopt and embrace new defenses against emerging and unanticipated attack modes. In order to ensure high resiliency and high performance in public and private networks efforts need to be concerted by administrators, service providers and equipment manufacturers. It is of great importance that citizens communicate with their government authorities online. No one should be allowed to shut down valuable e-government services. A more enlightened approach would be to ask all citizens to take responsibility for securing the Internet in their hands. Public awareness is the key in order to securely exist and succeed in the world of e-government.

REFERENCES

Barlow, J., & Thrower, W. (2000). *TFN2K—An analysis.* Retrieved from http://seclists.org/lists/bugtraq/2000/Feb/0190.html

Bysin. (2001). *Knight.c Sourcecode.* Retrieved from http://packetstormsecurity.nl/ distributed/knight.c

CERT. (2001). *CERT Coordination Center Advisory CA-2001-19 Code Red Worm Exploiting Buffer Overflow in IIS Indexing Service DLL.* Carnegie Mellon Software Engineering Institute. Retrieved from http://www.cert.org/advisories/CA-2001-19.html

CIAC Information Bulletin. (2001). L-040: The Ramen Worm. *Computer Incident Advisory Capability (CIAC).* Retrieved from http://www.ciac.org/ciac/bulletins/l-040.shtml

Cisco Systems, Inc. (2006). *Strategies to protect against distributed denial of service (DDoS) attacks* (Document ID: 13634). Retrieved from http://www.cisco.com/warp/public/707/newsflash.html

Computer Security Institute. (2003). *2003 CSI/FBI Computer Crime and Security Survey.* CSI Inc.

Computer Security Institute. (2004). *2004 CSI/FBI Computer Crime and Security Survey.* CSI Inc.

Criscuolo, P. J. (2000). *Distributed denial of service Trin00, Tribe Flood Network, Tribe Flood Network 2000, and Stacheldraht CIAC-2319* (Tech. Rep. No. , UCRL-ID-136939, Rev. 1.). Department of Energy Computer Incident Advisory Capability (CIAC), Lawrence Livermore National Laboratory. Retrieved from http://ftp.se.kde.org/pub/security/csir/ciac/ ciacdocs/ciac2319.txt

Cs3 Inc. (2005). *Defending government network infrastructure against distributed denial of service attacks.* CS3-inc.com. Retrieved from http://www.cs3-inc.com/government-ddos-threat-and-solutions.pdf

Dietrich, S., Long, N., & Dittrich, D. (2000). Analyzing distributed denial of service tools: The shaft case. In *Proceedings of the 14th Systems Administration Conference (LISA 2000)* (pp. 329-339), New Orleans, LA.

Dittrich, D. (1999a). *The tribe flood network distributed denial of service attack tool. University of Washington.* Retrieved from http://staff.washington.edu/dittrich/misc/ trinoo.analysis.txt

Dittrich, D. (1999b). *The Stacheldraht distributed denial of service attack tool. University of Washington.* Retrieved from http://staff.washington.edu/dittrich/misc/ stacheldraht.analysis.txt

Dittrich, D., Weaver, G., Dietrich, S., & Long, N. (2000). *The mstream distributed denial of service attack tool.* University of Washington. Retrieved from http://staff.washington.edu/dittrich/misc/mstream.analysis.txt

Douligeris C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: Classification and state-of-the-art. *Computer Networks, 44*(5), 643-666.

Fox News. (2002). *Powerful attack cripples Internet.* Retrieved from http://www.linux.security.com/content/view/112716/65/

Hancock, B. (2000). Trinity v3, A DDoS tool, hits the streets. *Computers & Security, 19*(7), 574-574.

Holden, S., Norris, D., & Fletcher, P. (2003). Electronic government at the local level: Progress to date and future issues. *Public Performance and Management Review, 26*(4), 325-344.

Householder, A., Manion, A., Pesante, L., Weaver, G. M., & Thomas, R. (2001). *Trends in denial of service attack technology* (v10.0). CERT Coordination Center, Carnegie Mellon University. Retrieved from http://www.cert.org/archive/pdf/DoS_trends.pdf

Howard, J. (1998). *An analysis of security incidents on the Internet 1989-1995.* PhD thesis, Carnegie Mellon University. Retrieved from http://www.cert.org/research/ JHThesis/Start.html

Insecure.org. (1997). *Ping of death.* Retrieved from http://www.insecure.org/sploits/ ping-o-death.html

Institute for e-government Competence Center (IfG.CC). (2002). *eGovernment: "First fight the hackers."* Retrieved from http://www.unipotsdam.de/db/elogo/ifgcc/index.php?option=com_content&task=view&id=1450&amp;Itemid=93&lang=en_GB

ITworld.com. (2001). *CERT hit by DDoS attack for a third day.* Retrieved from http://www.itworld.com/Sec/3834/IDG010524CERT2/

Karig, D., & Lee, R. (2001). *Remote denial of service attacks and countermeasures* (Tech. Rep. No. CE-L2001-002). Department of Electrical Engineering, Princeton University.

Leng, X., & Whinston, A.B. (2000). Defeating distributed denial of service attacks. *IEEE IT Professional, 2*(4) 36-42.

Mirkovic, J. (2002). *D-WARD: DDoS network attack recognition and defense.* PhD dissertation prospectus. Retrieved from http://www.lasr.cs.ucla.edu/ddos/prospectus.pdf

Mirkovic, J., Martin, J., & Reiher P. (2001). *A taxonomy of DDoS attacks and DDoS defense mechanisms* (Tech. Rep. No. 020018). UCLA CSD.

Moore, D., Voelker, G., & Savage, S. (2001). Inferring Internet denial of service activity. In *Proceedings of the USENIX Security Symposium*, Washington, DC (pp. 9-22).

SANS Institute. (2000). *Consensus roadmap for defeating distributed denial of service attacks* (Version 1.10). Sans Portal. Retrieved from http://www.sans.org/dosstep/ roadmap.php

Singer, A. (2000). *Eight things that ISP's and network managers can do to help mitigate distributed denial of service attacks.* San Diego Supercomputer Center (SDSC), (NPACI). Retrieved from http://security.sdsc.edu/publications/ddos.shtml

Sophos.com. (2002). *Indian sympathisers launch denial of service attack on Pakistani government.* Retrieved from http://www.sophos.com/virusinfo/articles/yahae3.html

Spafford, E. H. (1998). *The Internet worm program: An analysis* (Tech. Rep. No. SD-TR-823). Department of Computer Science Purdue University, West Lafayette, IN.

Specht, S., & Lee R. (2003). *Taxonomies of distributed denial of service networks, attacks, tools, and countermeasures* (Tech. Rep. No. CE-L2003-03). Princeton University.

Symantec. (2004). *Symantec reports government specific attack data* (Article ID 4927). Symantec.com. Retrieved from http://enterprise-security.symantec.com/publicsector/ article.cfm?articleid=4927

WindowsITPro. (2001). *Microsoft suffers another DoS attack. WindowsITPro Instant Doc 19770.* Retrieved from http://www.windowsitpro.com/Articles/Index.cfm? ArticleID=19770&DisplayTab=Article

U.S. Subcommittee on Oversight and Investigations Hearing. (2001). *Protecting America's critical infrastructures: How secure are government computer systems?* Energycommerce.house.gov. Retrieved from http://energycommerce.house.gov/ 107/hearings/04052001Hearing153/McDonald229.htm

Stein, L. D., & Stewart, J. N. (2002). *The World Wide Web Security FAQ version 3.1.2. World Wide Web Consortium (W3C).* Retrieved from http://www.w3.org/Security/Faq

Walters, R. (2001). Top 10 ways to prevent denial-of-service attacks. *Information Systems Security, 10*(3), 71-72.

This work was previously published in Secure E-Government Web Services, edited by A. Mitrakas, P. Hengeveld, D. Polemi, and J. Gamper, pp. 124-142, copyright 2007 by Idea Group Publishing (an imprint of IGI Global).