International Journal of Internet, Broadcasting and Communication Vol.8 No.2 55-65 (2016)
http://dx.doi.org/10.7236/IJIBC.2016.8.2.55

IJIBC 16-2-7

A STUDY OF DISTRIBUTED DENIAL OF SERVICE ATTACK ON GOVERNMENT INFRASTRUCTURE

Suk-Jin Kim[1] and Gisung Jeong [2*]

[1]Center for Advanced Image and Information Technology School of Electronics & Information Engineering ChonBuk National University, 664-14, 1Ga, DeokJin-Dong, Jeonju, Chon buk, 561-756, South Korea

[2]Department of Fire Service Administration, WonKwang University, Republic of Korea

E-mail: jgskor@wku.ac.kr

Abstract

Distributed Denial of service attack is one of the major threats nowadays especially to the government infrastructure that give huge impact to the reputation and interrupt the services and resource. Our survey start with brief introduction about DDoS attacks , we illustrate the trends and incident happened at government from various countries. We then provide an extensive literature review on the existing research about implication, types of attacks and initiative to defence against the DDoS attacks. Our discussion aims to identify the trends in DDoS attacks, in depth impact of DDoS attacks to government infrastructure, classification of attacks and techniques against the attacks. And we will use for a fire fight safety and management.

Keywords: *DDos, Infrastructure, Sensor network, Attacks, Vulnerability*

1. INTRODUCTION

We live in the world of electronic and internet services and these elements were provided by government. A local and state government is needed to take part in revolution of technology. Local and state government can use e-government technology or digital government which can provide convenience for citizens and organization to reduce waiting lines and acquire information. Moreover, e-government improves public service, propagate processes and license access to information. Digital government and e-government are mainly foundation on internet technology. Sometimes we face with vulnerability of internet infrastructure and danger of interconnectivity. Hence, for protection against DDOS attacks we must have an impression e-government service without interruption in web access and e-mail. The new kinds of attacks are (DDOS) or Distributed Denial of Service and this attack is executed on net services and resources [31].

Manuscript Received: Mar. 3, 2016 / Revised: Mar. 13, 2016 / Accepted: Apr. 2, 2016
Corresponding Author: jgskor@wku.ac.kr
Tel: +82-63-850-6398, Fax: +82-63-850-6907
Department of Fire Service Administration, WonKwang University, Republic of Korea

The attack is very dangerous and is able to control a huge numbers of computers by utilizing malicious software to launching Distributed Denial of Service attack. Several online websites such as Amazon, Google, Yahoo and e-bay and other business websites are available which could have serious subsequences. In many years ago, many government sites were interrupting by the attacks [32, 33, 34, 35]. As a result, many of research, spectrum analysis and methods to find the cause of such attacks are introduced. However the first denial of service attacks is started appearing and launching in 1998.

In general, denial of service attack is a significant threat for networking communication and infrastructure of critical information. In 2005, The UK National Infrastructure Security Coordination Centre (NISCC) and world Economic Forum (WEF) [36] were expressed respectively that denial of service attack could strike the critical national infrastructure and caused to crash the infrastructure of critical information. Reaching an especial network resource is intended for prohibiting legal users by distributed denial of service attack and in 1980, first paper was written from networking research community [9]. Indeed, first statement of DOS in operating system was provided in 1983 and in 1985.

According to Morris, finding the original of packet is no prevision in the IP (internet protocol) [38,39]. Nowadays [39,40], most of computers have a firewall and antivirus software and its create difficulty to the attacker but some of the computer do not have firewall or update antivirus software. Attacker sends traffic concurrently to the victim computer (figure 1). Consequently, the number of legal client cannot connect to link or routers. For instance, the kinds of victims are e-commerce websites, news websites, corporate networks, banks and governmental websites. The first DDOS attacks occurred in the summer of 1999[41] and in February 2000 the main DDOS attacks was waged against yahoo.com. This problem is caused cripple web site and lost the significant cost, users and revenue of advertise [42]. The others attacks occurred in 2002 against domain name system (DNS) service.

This attack enable change to the logical addresses such as yahoo.edu to IP address, so users can use and remembered the name instead of numbers when they can connect to website. If 13 roots of DNS were breakdown, it could be problems for World Wide Web (www) and if the 7 of 13 roots server was shut down for one hour , it could be remained great damage. Totally we must the check all of internet services in minute. In this paper, we want to describe the problems of attacks, impact, incident, initiative against on DDOS and future on hold.

2. TRENDS AND INCIDENTS

The increase of usages and features of Internet has changed the trends of DoS attacks [1]. Internet is important as a platform to the government to deliver services and information to the community and the nation and it help increase the collaboration and sharing information and knowledge [2].Earlier, most of the attack are 1-tier attack known as Denial of Service [4],nowadays, attacks are using 2-tier or 3-tier known as Distributed Denial of Service [4] have become one of the serious attacks that cause million of losses, damage and reputation not even to the firm or government agencies but towards the political and economics of the country. SYN FLOOD [1], SMURF[2], BRUTE FORCE AND SEMANTIC ATTACK [3], AGENT-HANDLER AND IRC-BASED [4] are an example of DoS and DDoS type of attacks.

Until end of year 2010[15], DDoS attacks sizes have increasing very fast every year, most of the attacks are targeting application layer and network infrastructure. HTTP [16] and DNS [17] still on the top for application layer attacks by DDoS. Recently SMTP, SIP/VOIP and HTTPS attacks also took place and increasingly. Most of the agencies had an experienced firewall and IPS failure where 49% of the agencies had an experience facing the failure. Proportion attack over 10 GB per second has grown up 319% from year

2009 to year 2010, proportion of targeting port 80 also increased from 19.6% in year 2009 to 31 % in year 2010. DDoS attacks not only targeting port 80 but also port 53 and the proportion has boost. The proportion sizes of attacks targeting port 53 have increase 885% over 10GB/sec.

For second quarter of the year 2011 regards DDoS attacks [14], USA and Indonesia leading the attacks with percentage of 5% and Malaysia contribute 3% from the total distribution of the attacks. Online shopping donate 25% from the activity that cause the DDoS attacks to the agencies, 20 % of the attacks site are from gaming site and 11% of the total attacked site are government sites . Nowadays, DDoS attackers targeting government sites are not for profit or any benefit but more to showed their protest and skill against any behavior towards the government. The largest attacks are 60 days, 1 hour, 21 min and 9 second and the uppermost number of attacks adjacent to a single site is 218.

DoS/DDoS attacks is not a common threats, it's already became threats before year 2000[1], but it become more serious after the usage of internet become more important and most of the government agencies rely on internet for online transaction and deliver services to the citizen. DDoS attacks tools [4] have caused Iran Government website server crash and the website page have problem to view the content. The attacks can cause hazardous and traffic to the government network infrastructure [8] and stop all the services and resource that available for the legitimate user to access. South Korean Government and major firm [19] has been attacked uses virus in zombie computers and create traffic within all the sites. Malaysia government website, www.malaysia.gov.my [20] and Japanese Government site [10] attacks by DDoS have caused the services and reputation of the countries drop down. Japanese claimed that the attacks has political motive and the attacks using large amount of email cause the system collapse. DDoS attacks to the Swedish Police [11] and Swedish Signals Intelligence Agency (FRA) [12] website by packet flood and massive attacks have effect the website offline and services interrupted. South Korean Government [13] lost 4-5 billion USD cause by the DNS, ICMP and HTTP GET attacks to the government site.

Most of the government agencies have experienced this type of attackers either countries with a very good well ICT Security experts or the countries with very poor ICT awareness among citizens. The incidents not only give huge losses to the profit and reputation of the countries but also cause damage to the data, hardware and network infrastructure of the agencies. U.S Government, one of the most countries that consists of many expert in security, face challenges with the highest rank of the country that deal with DDoS attacks [18]. U.S Government experience attacks from Israel that attacks pentagon computers and in year 1999, US government website www.whitehouse.gov down for three days and US embassy at Beijing China was hacks with the racist slogan at the website . Besides that, 400 000 zombie computers launch by the attacks and 100 computers have been attacks at Defense Department, Army, Air Force and NASA in year 2001.

3. IMPLICATION OF ATTACKS

DDOS Attacks give a big impact to the government and firm, it's make organization suffer a very huge financial losses, beside interrupt all operations inside the organization [21]. The attacks target critical and valuable network assets and become major threat to online banking transaction.

In this paper, we will focus into impact of DDoS Attacks to government infrastructure. There is no specific paper that discuss about the implication of the attacks to the government infrastructure. General impact to the government is bad reputation especially government with a high security technology and have a lot of security experts [22] . Most of the attacks to the government site not with the purpose to financial losses, it's more to political agenda and protest among the citizens or the other countries. But nowadays, we have to think seriously how to protect the government infrastructure, motive of the attacks mostly because of political agenda and protest but it's can cause very big impact to the government, for example in Malaysia, Malaysia Government Website is the main website for all the citizens that link all the agencies services and resource in the web. It's allowing the citizens to pay summons, renew road tax, checking land fees and others more. The government ICT Security must be aware government nowadays not only act as agencies that given one way information to the citizens, but also interact actively with the firm, private sector and all the other client all around the world.

DDoS attacks significantly cause threats to the infrastructure [15], 60% infrastructure outage due to failure by the attack, 40% infrastructure outage due directly by DDoS attack, 48% cause services offline and cannot be access by legitimate user and 38% of the attacks cause difficulty to the infrastructure. Attack to the critical infrastructure repeat again and again [23], the attack also takes control of data computer network own by the government and distributed the attack to the other branch in many countries. 29% of the correspondent [23] experience multiple times of attacks every month and 64% from the total attack give big impact to the operation of the government. The Attorney General's Department in the Federal Government Australian has recognized the infrastructure and conveniences the "physical, supply chain, information technology and communication networks which, if destroyed, degraded or made available for a long time, will have a major impact on the social and economic well-being of the nation or affect the ability of Australia on the behavior of national defense and national security [56].

Generally, the impact of the DDoS Attacks to the government website is affecting the website which the website loading very slow, server response very slow and transaction failure and its cause client complain. Some of the government agencies are responsible to collect revenue such as land office, police department and road transport department. The impact of the attack to the government not only about reputation but also relate with the revenue to the government. Form our research about DDoS Attacks on government infrastructure, we have found out that most of the paper is discuss about different types of attack and technique to prevent organization from the attacks. Specific discussion about the impact to the government infrastructure and how to defend government infrastructure are rarely to found. Cs3.Inc [21] discuss about the initiative that have taken to defend the government network infrastructure but the discussion about the impact to the government infrastructure should cover from many area, not focusing only to the government infrastructure. Wikipedia [24] describe infrastructure from two type of government infrastructure. The first type is 1) hard infrastructure and other one 2) soft infrastructure.

From our view, if we want to talk about DDoS attacks on government infrastructure, we should consider to separately study the impact of the attacks specifically to the two types of infrastructure, only after that we can find the effective ways to defend the government infrastructure. Below, our group list out the type of infrastructure and the area cover so later if given the best opportunity, the study in this area should be focus.

3.1 Hard Infrastructure

Hard infrastructure [24] is define as huge physical network that need to allow fixed asset, software and control system running. Hard infrastructure consists of transportation infrastructure, energy transportation, water management infrastructure, communication infrastructure, earth monitoring and measurements network infrastructure and solid waste infrastructure. Transportation infrastructure contributes 50% from the total type of infrastructure that has been attacks [23] and water management infrastructure cover 17 % from the infrastructure that has been attacks. From the statistics, the attacks not only focus to the network infrastructure but every type of infrastructure going to be attacks and the threats open to the wide financial losses.

3.2 Soft Infrastructure

Soft infrastructure is combination between physical and non physical assets [24] and the main function is to deliver specialized system to the community. The Accounting system, Legal system and Cultural attitude [25] should be consider when we are talking about the impact of security and threats of attack to the government infrastructure. Governance infrastructure such as emergency service, military, law enforcement, Economic infrastructure including financial, logistic, social infrastructure and Cultural, Sport and Recreational infrastructure [24] strictly will be open to this types of attack and cause damage and losses to the infrastructure.

4. CLASSIFICATION OF DDOS ATTACKS

This part we show the classification of DDOS attack and different type of attacks on Government infrastructure:

The taxonomy of distributed denial of service attacks shown in figure 1, [43] and propagation into depletion of broadband and resource depletion attack. In this propagation, attacker moved the victims with large traffic that avoid amplify and legal traffic by sending message to IP addresses. In favor of tie up the critical resource, attackers use the victim that unable to process the services. Hence, this is done by exploiting the TCP protocol.

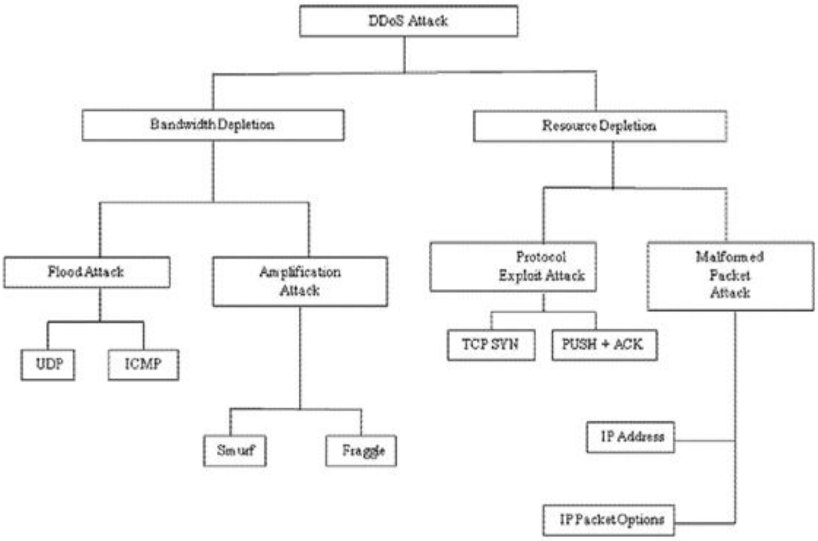

Figure 1. DDos Attack Classification

Bandwidth flood attack to congest government network infrastructure, the attacks , common types of attack are UDP flood and ICMP flood and the service can resume after attacks. Protocol Exploit Attacks attack on vulnerability on protocol or application, common types of attack are TCP SYN flood, HTTP Get Flood and DNS Query Flood and the service may not resume after the attack.

Table 1. Comparison of DDOS Attacks Tools

S.NO.	Tool name	Passible attacks	Packet format used to launch an attack	Chanel encryption	Model used
1.	Trinoo [41]	Bandwidth Depletion, Remote Buffer Overrun Exploitation	UDP	Yes	Agent Based
2.	TFN (Tribe Flood Network)[49]	Both Bandwidth and Resource Depletion	UDP,TCPSYN, ICMP echo request And directed broadcast	No	Agent Based
3.	TFN2K [50]	TARGA and MIX attack	UDP,TCPSYN, ICMP	Yes (KeybasedCAST-256 algorithm)	Agent Based
4.	Stacheldraht [51]	Both bandwidth and resource Depletion	UDP,TCPSYN, ICMP echo request And directed broadcast	Yes (Symmetric Key)	Agent Based
5.	Mstream[52]	Bandwidth Depletion	TCP with ACK flag set, ICMP, and TCP RST	No	Agent Based
6.	Shaft[53]	Bandwidth and Resource Depletion	UDP,TCP,ICMP	No	Agent Based
7.	|Trinity[54]	Both Bandwidth and Resource Depletion	UDP,TCPSYN,TCP With ACK flag set TCPNUL, and TCP RST	No	IRC Based
8.	Knight[55]	Both Bandwidth and Resource Depletion	SYN, UDP, and Urgent pointer Flooder	No	IRC Based

Table 1 show the comparison of DDoS attacks tools. Attackers can use ID launching and spoofing the source IP addresses, furthermore using the NMAP [44] for identifying the vulnerable systems by scanning the TCP and UDP ports. Most of the tools can download from the internet without any cost and NMAP is powerful tool for utilization of operating system (OS) in systems.

SANS Internet Storm Center reported [45] that Windows machine that are not patches have survival time 78 minutes before it compromised. Most DDOS attacks can be controlled uncertain systems which are dependent on the abundance of connected to the botnet work. This patch is directly related to the weak process of survive time by this activity and increased the humble and attackers are developing and deploying forces for the vulnerabilities released

5. INITIATIVE TO DEFENSE DDOS ATTACKS

There is a lot of initiative and techniques have been study and implement to defence the organisation from DDoS Attacks. Different type of techniques have been discuss and implement, our group have summarize the techniques to defences from the attacks into three prevention techniques, detection techniques and response techniques.

5.1 Prevention Techniques

Denial of Service Prevention [3] such as improve network and host configuration to protect the infrastructure from the attacks through source address spoofing, network router is configured to make sure spoofed address can't transit between sub network. Implementation of protective overlay networks, network enforceable capability, and resource allocation model, improve protocol and applications also can prevent the attacks from occur. Secure overlay [28] suggests hiding the ip address, end-host controls and avoiding new vulnerabilities to prevent infrastructure from the flooding attacks cause by DDoS attacks. Beside the technical prevention, law enforcement must be considered [29]. Computer crime and Intellectual property section of the US Department of Justice is one of the law enforcement to prevent from the DDoS attack. Hang Chau [29] focus on prevention against SMURF [30], SYN FLOOD [30] and DNS attack including prevent from the root server configuration, router configuration and end-to-end connection.

5.2 Detection Techniques

Detection strategies [4] divide into three main strategies, signature detection and anomaly detection or hybrid detection, combination of both. George Loukas [1] mention the detection technique using ART, RBFNN, TRA, Fuzzy techniques, wave-let method and CUSUM method. Stamping mechanisms [9] could defence the attacks through get rid of the distributed IP spoofing and packet format problems. Blackhole , router and firewall, IPS, Content Delivery Network (CDN), ISP filtering and Clean Pipe are among the techniques could be considered for detection to defend the government infrastructure from the attacks. Government Agencies using cloud computing as their infrastructure network can use Cloud Tracing and Filtering (CTF) as one of initiate to defence ddos attacks [5]. Government agencies can use CTF to detect and filter any request services and discover the source of attackers.

5.3 Response Techniques

Denial of Service Response is important as countermeasure to response to the attack. Content distribution network (CDN) [3], pricing mechanism [26] and trace back techniques [27] are an example of the response techniques

Table 2 show the comparison between current and future trend of the attacks. For future attacks most of the attacks are cloud and shared infrastructure including web services because in the future trend of cloud computing among organization will be increasing. Government has to look into the overall of infrastructure to make sure the attacks not harm and given serious impacts to the government infrastructure. For further action, research about the impact of DDoS attacks to the types of government infrastructure should be the focus of the research; the findings of the impact will be very enormous assist for extensive research on prevention and detection for DDoS attack

Table 2. Comparison current and future trend of DDoS Attacks

Current	Future
Propagation of autonomous and larger bot network	*New technology have attacks*
Markets of bot network which are increasingly sophisticated in nature	*Application of DOS layer*
Peer to peer bot network	*DOS traffic have behavior realistic*
Using bot network by encrypted communications	*Infrastructure of anti-DOS against attacks*
Government infrastructure against attacks for purposes of political	*Attacks against SCADA systems*
DOS using by organized crime	*The 'cloud' and shared infrastructure against attacks*
Virtual servers against attacks	*Web services against attacks*
Increasing sophistication of malware and malware packaging	

6. CONLUSION

According to previous discussion, distributed denial of service attacks are made by loss of security mechanisms and intrinsic flaws in designing of internet in many computers system. In future, we have more problems because per years many computers are being connected to the internet. Therefore, in future we will have more hosts that most of them have permanent IP addresses by name users on a bandwidth connection. We have the sort of worm such as the SQL slammer worm and the code red worm are highly attacking and they can damage collateral. The system can connected to the attacked and block them.

Accordingly, we assume that if when ATM machines working during the time is stopped by slammer worm attack. It is very terrible, when we think about it. Later, this worm can be warfare between countries. Super worms [46] broadcast through the internet each minute with spread of the slammer worm. These worms can spread faster in the internet and system administrator cannot prevent them. Hence, we need more research for preventing them.

Future research will have to face the effective challenge combining the suggestion of diversity for DOS finding and response procure to strength and weakness in architecture. We believe that increase the security software before the customer request to it. Hope the government helps the society and spends more money for secure software prior extension the worm in internet.

REFERENCES

[1] Georgio Loukas and Gulay Oke, "Protection Against Denial of Service Attacks: A Survey," 2002.

[2] Howard F. Lipson, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues," 2002 .

[3] Jason Smith, " Denial of Services :Prevention, Modelling and Detection", 2007.

[4] K.Omirston and MM Elof , "Denial-of-Service and Deistributed-Denial-Of-Service On The Internet," .

[5] Fan Lin, Wenhua Zeng and Yi Jiang, "A Cloud Tracing and Filtering Framework for Defensing Against Denial of Service Attacks," *International Journal of Digital Content technology and its Apllication*, vol. 4, Number 9, December 2010.

[6] Darren Anstee, "DDoS Attack Trends Through 2010, Infrastructure Security Report and ATLAS Initiatives," 2011.

[7] R.Benjamin, B.Gladman and B.Randell, "Protecting IT System from Cyber Crime,"*The Computer Journal*,Volume 41,Number 7,1998.

[8] Oleksii Ignatenko , "Denial of Service Attack in the Internet: Agent-Based Intrusion Detection and Reaction," 1999.

[9] S.S Nagamuthu Krishnan and Dr. V. Saravanan, "DDoS Defense Mechanism by applying stamps," *IJCSNS*,Vol.9, No.8, 2009.

[10] Mary Barifield, "Hackers Attack Japan Government and Mitsubishi," *http://threednews.com* , September 21 2011.

[11] Dan Goodin, "DDOS Attacks Topple 40 Swedish Sites," *http://www.theregister.co.uk*, October 2009.

[12] John Leyden, "Swedish spooks knocked offline by hack attack," *http://www.theregister.co.uk*, November 2009.

[13] John Leyden, "South Korea Blitzed by DDOSers," *http://www.theregister.co.uk*, 4 Mac 2011.

[14] "DDOS Attacks in Q2 2011," *http://www.securelist.com,"* 29 August 2011.

[15] Darren Anstee, "DDOS Attack Trends Through 2010 Infrastructure Security Report and ATLAS Initiative," *Arbor Networks Worldwide Infrastructure Security Report, Volume VI*.

[16] Patrick Chang and Lori Mac Vittie, "The Fundamentals of HTTP," *F5 White Paper*,2008.

[17] Incognito Software, "Understanding DNS (The Domain Name System," January 2007.

[18] Focus Editor, "Top 10 U.S Government Web Break-Ins of All Time," *http://www.focus.com*.

[19] Infosecurity.com, "South Korean Government agencies hit by DDOS Attacks," *http://www.infosecurity-magazine.com*, 4 March 2011.

[20] "Anonymous Group Hits Malaysian Government Hard With DDOS Attacks", *http://dos-attacks.com*, 16 Jun 2011.

[21] CS3.Inc, "Defending Government Network Infrastructure against Distributed Denial of Service Attacks," October 2002.

[22] Frank TSE, "What is DDOS and Mitigation Strategies," *Nexusguard.*

[23] Stewart Baker, Shaun Waterman and George Ivanov, "In The Crossfire Critical Infrastructure in the Age of cyber War," *McAffee*, 2009.

[24] Wikepedia, "Infrastructure," *http://en.wikipedia.org/wiki /Infrastructure*.

[25] William A. Niskanen , "The Soft Infrastructure of a Market Economy," *Cato Journal, p. 233-238.*

[26] X.Wang and M.K.Reiter, "NADIR: an automated system for detecting network intrusions and misuseDefending Against Denial-of-Service Attacks with Puzzle Actions," *In Proceedings of the 2003 IEEE Symposium on Security and Privacy Security*. IEEE Computer Society, 2003.

[27] S.Savage, D.Wetherall, A.Karlin and T.Anderson, "Practical Network Support for IP Traceback," *IEEE/ACM Transactions on Networking (TON)*.

[28] Daniel Adkins Karthik Lakshminarayanan Adrian Perrig Ion Stoica, "Towards a More Functional and Secure Network Infrastructure ,".

[29] Hang Chau, "Network Security-Defense Against DOS/DDOS Attacks,".

[30] Hangzhou H3C Technologies Co.Ltd, "Attack Prevention Technology White Paper,".

[31] Vebjørn Moen, Andr´e N. Klingsheim, Kent Inge Fagerland Simonsen, and Kjell Jørgen Hole," Vulnerabilities in E-Government,".

[32] CNN. Cyber-attacks batter Web heavyweights, Feb 2000, http://www.cnn.com/2000/TECH/computing/02/09/cyber.attacks.01/index.html

[33] CNN .Immense. Network assault takes down Yahoo, February 2000, http://www.cnn.com/2000/TECH/computing/02/08/yahoo.assault.idg/index.html.

[34] Netscape. Leading web sites under attack, February 2000, http://technews.netscape.com/news/0-1007-200-1545348.html.

[35] CERT coordination center. Denial of Service attacks, http://www.cert.org/tech_tips/denial_of_service.htm

[36] National Infrastructure Security Coordination Centre, " Botnets - the threat to the critical national infrastructure. Briefing 11a/2005," October 2005.

[37] Global Risk Network. World economic forum global risk report 2006,
http: //www.weforum.org/en/initiatives/globalrisk/.

[38] Gilgor V, " A Note on the Denial-of-Service Problem," *Proc. Symp. Security and Privacy* , 1983, pp. 139-149.

[39] Georgios Loukas and Gulay Oke, "Protection Against Denial of Service Attacks.," *Intelligent Systems and Networks Group, Imperial College*, 2009.

[40] Morris R.T, " A Weakness in the 4.2BSD UNIX TCP/IP Software," *Computer Science Technical Report*, 1985.

[41] Paul J. Criscuolo," Distributed Denial of Service Trin00, Tribe Flood Network, Tribe Flood Network 2000, and Stacheldraht CIAC-2319,"February 14 2000.

[42] “Yahoo on Trial of Site Hackers”, http://www.wired.com/news/business/0,1367,34221,00.html

[43] Stephen M.Specht and Ruby B.Lee, "Distributed Denial of Service: Taxanomies of Attacks, Tools and Countermeasures," September 2004.

[44] Nmap Stealth Port Scanner Introduction,
http://: //www.insecure.org/nmap/.

[45] SANS,2006 Survival Time History, http://isc.dshield.org/survivalhistory.php

[46] Vern Paxson, Stuart Staniford, and Nicholas Weaver, " How to own the Internet in Your Spare Time,"*11th USENIX Security Symposium,*2002.

[47] Security Privacy-Silver Linings in the Cloud,
http://books.google.com.my/books

[48] "Managing Denial of Service (DOS) Attacks,"*Summary Report for CIOs and CSOs*, December 2009.

[49] D.Dittrich, "The Trible Flood Network Distributed Denial Service Attack Tool," October 21.

[50] J.Barlow, W.Thrower, TFN2K an Analysis, http://security.royans.net/info/posts/bugtraqddos2.shtml>.

[51] D.Dittrich, "The_Stacheldraht_Distributed Denial of attack tool,"1999.

[52] D.Dittrich, G.Weaver, S.Dietrich and N.Long, "The mstream Distributed Denial of Service Attack Tool" May 2000.

[53] S.Dietrich, N.Long, D.Dittrich, "Analyzing Distributed Denial Services Tools:theShaftCase,"*14th Systems Administration Conference*.

[54] B.Hancock, "A DDOS Tool, Hits the Streets," *Computer Security*, 2000.

[55] Continuing Threats to home users, http://www.cert.org/advisories/CA-2001-20.html.

[56] Trusted Information Sharing Network: About Critical Infrastructure, *http://www.tisn.gov.au*.