Seminar on Internet Technologies - Summer 2008

Denial of Service and Spam in Online Communications

Swen Weiland

October 6, 2008

Supervised by Prof. Dr. Xiaoming Fu and M. Sc. Niklas Neumann
Computer Networks Group
Georg-August-University of Göttingen

Contents

1 Denial of Service

1.1 Introduction

The therm "Denial of Service" (DoS) defines a class of remotely initiated attempts to make a computer network resource unavailable or unusable to its intended users or intended purpose. Generally, these attempts are coordinated and concentrated attacks on a single service or network resource from multiple sources. Attacks from multiple sources are named more precise as "Distributed Denial of Service" (DDoS) attacks. Also attacks from a single but better equipped host such as a host with higher bandwidth are possible. In most cases a DoS attack is enhanced by deploying it using flaws in network protocols or topology. Some of them are further described in section 1.2.
Attacks are motivated by preventing an Internet site or service from functioning efficiently for a defined period or indefinitely. Sometimes an attack is escalated so much that it prevents a service from functioning at all! Typical targets for DoS attacks are sites or services hosted on high-profile servers such as banks, search engines, DNS servers or popular websites.
Unlike from normal attacks, DoS attacks cannot be used to to compromise a system by stealing passwords or gain access at all but they can be part of such an attack. For example a DoS attack can be used to distract from the actual attack or delay responses from the original service to inject own data. The second scenario can be applied for the Domain Name Service (DNS). A DNS server is overloaded with request which delays its responses and gives an attacker time to send a manipulated answer for regular requests with a spoofed origin. Spoofing the origin Internet Protocol (IP) Address or using hijacked machines as drones for an DoS attack is very common.
Manipulating the header fields of an IP packet (e.g. the origin address) is either used to hide the attacker and make it harder to track him down or to introduce a more effective method for a DoS attack. Sometimes both facts apply. More effective means to amplify an attack in quantity or to increase its impact by using anomalies or software errors in network protocols or topology. This can lead to increased amount of processing time for each request or packet introduced by a DoS attack and therefore reduce the capacity of a network resource.
For defense, a service provider has to shutdown the network resource under attack or block the traffic from a DoS attack at his border routers. This makes the node unreachable or at least hardly reachable for regular traffic, because it is difficult to distinguish between DoS traffic and regular traffic. Using drones makes it even harder for an ISP to identify and block such traffic. Drones can be spread all over the world and their count may vary during

an attack. Many different sources are hard to block and DDoS attacks utilizing drones are very common todays. In the following section 1.2 some attacks are described and in section 1.3 some countermeasures are given.

1.2 Attack Vectors for DoS

1.2.1 Flooding

Flooding is a very basic method of attack that saturates the network link of a network resources with external communication or communication requests. As result, the network resource responds only very slowly to legitimate requests because its network link is congested and/or the high amount of requests consumes all processing power. By creating as many as possible communication sessions also the memory resources are tied up. Some well known and common attacks are as follows:

- **UDP Flooding**
  Several thousands of bogus UDP packets are send to a network node, which simply exhausts the bandwidth of its network link. By using UDP for the attack, no connection setup procedure to transfer data is needed because UDP is a connectionless and stateless protocol. This attack is addressed by CERT advisory [CA-1996-01]. Additionally to the bandwidth exhaustion, for each packet the victim of the attack has to determine what application is waiting on the destination port. Randomizing the destination port is a common method to make it a little harder for the victim to process the packets. If no application is waiting on the port, a Internet Control Message Protocol (ICMP) packet is generated to signal the sender that the destination is not reachable. The sender has in most cases a forged source address. Generating the ICMP message additionally stresses the network link of the victim node. Reaching a certain limit of traffic the victim network node will go down.

- **SYN Flooding**
  A network node providing a service which is delivered with TCP is made unavailable by blocking it with unfinished connection requests. This attack is addressed by CERT advisory [CA-1996-21]. TCP does a three-way handshake during connection establishment and this type of attack takes advantage of this. First step of this Handshake is sending a SYN packet by the initiator of the connection which is replied by a SYN-ACK from the corespondent node. In this case our victim which provides a service. After these two steps the connection is considered as “half-open”, because only the third and last step is not proceeded yet. The third step is an ACK which is sent by the initiator, but this is skipped by the attacker. By creating as many “half-open” connections as the service can handle it is not reachable any more.

- **Internet Control Message Protocol Flooding a.k.a. Ping Flooding**
  Ping is the name for ICMP echo service. Usually this service is used to test the reachability of a network node. An ICMP Echo Request is answered with an ICMP Echo Reply. If no mechanisms are in place to process a huge amount of ICMP Echo Request in a short time, the network link of the victim is saturated. This attack does not use any enhancement which makes it quite ineffective. Anyhow this attack shows an impact if the traffic of the victim is charged by volume.

1.2.2 Logic or Software Attacks

Each attack of this class of attacks is using abnormal behavior in software or hardware as enhancement, which is created by software errors or use cases nobody has thought of before. They focus mainly on flaws in Internet Protocol (IP) Stacks in popular operating systems like Windows or Linux. These flaws can be exploited by sending modified IP packets to create a data stream which is not compatible to the protocol standard. Not every exceptional behavior is handled in every IP Stack implementation and therefore it crashes or can be used to hijack a system. The IP Stack is in most cases part of the operating system and runs as privileged code. This makes it a powerful attack and a good reason why all of these mentioned attacks got fixed very quickly.
Using exceptional behavior in the IP Stack is not always necessary. Just modifying a single field like the source address of a packet is sometimes sufficient. This called "spoofing" and hides at least the source of an attack but for this class of attacks it is mostly used for enhancing or amplifying an attack.

- **Disconnect a MODEM with Ping**
  This attack described in [Ruef] and [Mittner] is not that known or famous like the next one, but it involves common hardware which was common for a long time all over the world. From my personal experience i know that the attack was able to disconnect dial up connections of a small city during a few seconds. This was limited to a single Internet provider at a time, because only in that case were the IP addresses very close together which make potential victims with a dial up connection guessable.
  During the 1970s, the American company Hayes developed a standard command set for telephone line Modems. This command set, also known as AT-commands, is supported by nearly any modern Modem. After dialing, the Modem switches from command mode to data transfer mode. For switching back from data to command mode(e.g. for hanging up the telephone line) the escape sequence "`+++`" is send to the Modem. Escape sequence and commands must be send from the PC to the modem. For the receive direction they are ignored. Now comes Ping into play, a Ping is normally echoed by the pinged host. The attacker sends a ping request to the victim with "`+++ATH0`" in the payload. This character sequence switches the Modem to command mode and

"`ATHO`" hangs up the telephone line. Nowadays, this attack is not a thread anymore because telephone line Modems were replaced by Digital Subscriber Lines(DSL).

- **Ping of Death**
  In 1996 this nearly famous attack came up. It gained its popularity from its simplicity and from the huge amount of affected systems. These affected system were versions of Unix, Linux, Mac, Windows and some embedded systems like routers or printers. At that time the attack could be delivered by standard system tool "`ping`" or specialized tools. Basically, the attacker sends an oversized ICMP echo request to the victim.
  As in RFC 791[1] defined, an IP packet uses a 16 bit field in its header to describe the total packet length. Oversized means larger or much larger than $(2^{16} - 1)$ bytes including the IP header, which is the maximum value for the header field and 65,535 as number. To send such a large packet, the underlying layer has to fragment the packet. The receiver, who is also the victim of the attack, needs to reassemble the the packet and since the IP packet is bigger than the maximum allowed size this fails due to a buffer overflow. An buffer overflow could cause a reboot, a kernel panic, a frozen system and sometimes even having no effect at all.

- **Smurf Attacks (ICMP Broadcast)**
  Smurf is an attack which floods a target host with ICMP echo messages. Reason for beeing in this class of logic attacks and not in the Flooding class is that the ICMP echo messages are amplified in count. A use case that probably nobody thought of before and is addressed by CERT advisory [CA-1998-01]. Amplification is achieved by sending an ICMP echo request to a network broadcast address. All network nodes of a certain network respond to the broadcast network address. This means if a ICMP echo request is sent to a broadcast address, all connected nodes reply with a ICMP echo reply to the request. One request is multiplied in count by the number of nodes replying to the broadcast address. To direct the replies to a victim, the source address of the ICMP request is spoofed and replaced with the address of the victim. During the late 1990s many IP networks would participate in Smurf attacks but today only very few networks remain exploitable for the Smurf attack. The change came by making the administrators aware of this attack and changing the default policy in Cisco routers to not forward packets addressed to broadcast addresses in the year 1998.

- **Fraggle Attacks**
  The Fraggle attack is called the brother of Smurf by [Ruef], because it works the same way except using another network service. Instead of sending ICMP echo messages it sends UDP packets to port 7, which is the "`echo`" service. There is also a variant which sends packets to port 19, which is the "`chargen`" service. It is known, that the exploit source code for Fraggle and Smurf has the same author.

[1] RFC791 - Internet Protocol

- **Teardrop Attack**
  Teardrop is another attack that exploits a bug in the IP re-assembly and is addressed in CERT Advisory [CA-1997-28]. Known variants of Teardrop are `targa`, `SYNdrop`, `Boink`, `Nestea Bonk`, `TearDrop2` and `NewTear`. An attacker sends two overlapping fragments of a IP packet that cannot be reassembled properly by manipulating the offset value in the IP packet header. With this attack an attacker can crash a vulnerable system or make it unreachable. Normally IP fragments are sequentially and can be reassembled by their offset value. For the Teardrop attack the offset value of a fragments points into another fragment. They overlap. This creates a flaw in the IP stack and crashes the system.

- **Land Attack**
  The Land attack is also addressed in CERT Advisory [CA-1997-28]. It creates a "loop" which eats up all the processing power and causes a system to crash or freeze. An attacker initiates a connection from the victims host to itself by sending a spoofed TCP SYN packet with the victims IP address as source and destination address. Further, the packet is addressed to an open port of the victim but it also has the same port as source port. This causes that the victim host replies to continuously. Popular target services for this attack are again the echo port 7 and the chargen port 19, but also services like SNMP can be exploited for this attack. It was actually first discovered in 1997 and had a comeback many years later in operating systems such as Windows Server 2003 and Windows XP SP2.

1.3 Detecting DoS Attacks and Countermeasures at ISPs

Accordingly to [Czmok] the amount of DDoS attacks has increased about 10 percent in the first half of the year 2002. Most of the attacks utilized a bandwidth smaller than 50 Mbps/s, but a few of them were 10 times higher. Also the amount of non-spoofed attacks from hijacked computers, called "zombies", has increased. These "zombies" are created by spreading viruses and trojans which network themselves together. Zombies are remotely controlled over the zombie-network and then used for the DDoS attacks.
Prof. Dr. Claudia Eckert [Eckert] classifies the defense against DoS in preventive and reactive defense measures and these are defined as follows.

- **Preventive defense**
  Preventive defense has two goals. Prevention against attacks before they can take effect on a system or the prevention of DoS conditions on an attacked system. To reach these goals it is necessary to keep a system always up to date by always installing the newest security patches and network protocol fixes. Further more, an Intrusion Detection Software and a Network Firewall needs to be installed. For protocol design

it makes sense that intense processing like cryptography is done on the client side and not on the server. This makes the server less vulnerable to attacks which try to steal processing power. The second goal of preventing DoS conditions is archieved by limiting bandwidth with quality of service methods or buy more powerful hardware with load sharing to have redundancy in capacity. Overall these measures would shrink down the amount systems of systems that can be used as zombies and therefore DDoS attacks are less effective.

- **Reactive defense**
  Before having a reasonable reaction to an attack, the attack needs to be identified. This is done by pattern recognition, anomaly detection or combinations of both. By comparing network data with patterns of already known attacks, these attacks can be identified with a high probability but unknown attacks cannot be identified. The anomaly detection compares with a standard network status and rates the differences to the standard. If the differences reach a certain threshold it is assumed that an attack is in progress. It is very hard to define the threshold to minimize false alarms and maximize the detection of actual attacks. Hybrid of both methods are used in Intrusion Detection Systems. The reliable pattern recognition is used to detect the attacks and the anomaly detection creates new patters for the pattern recognition. It can be problematic to use the fully automatic created patterns, because an attacker could use the anomaly detection to create a pattern for legitimate network traffic and so the protection becomes the DoS attacker.

The following subsections gives some examples for detecting DoS attacks and countermeasures used by Internet Service Providers (ISPs).

1.3.1 Pushback

This group of methods propagates the knowledge of an attack with an overlay network to the upstream or border routers to take measures against a DoS attack. These measures are throttling or blocking the network traffic of the attack. The overlay is implemented by propagate the information of an attack to all neighbor routers. Upstream and border routers are chosen to react against the attack as early as possible in the network and to keep the attack traffic outside of the own network. Detection of an attack is triggered by a rate limit and only the attack traffic is filtered.

1.3.2 IP Traceback

These approach extends the IP by adding information to the IP packet header, which makes it possible to trace back the source of the packet. This additional information describes the way of a packet through a network. Traceback is very useful if the attacker used a spoofed

IP source addresses. Many of the attacks generate non spoofed traffic. For non spoofed traffic Traceback is only additional overhead, because the source and route of a packet can be determined by the routing tables.

1.3.3 CenterTrack

Accordingly to [Czmok] CenterTrack is used by the Uunet ISP. This approach implements an overlay network with an IP/MPLS tunnel, which can be transparently put on a specific network flow. It is designed to track down the source of an attack by utilizing realtime monitoring. Interesting datagrams are rerouted to special tracking routers for more detailed investigations. These tracking routers are using network statistics, sniffers and BlackHole-BGP.

1.3.4 BlackHole-BGP

BlackHole-BGP is part of the CenterTrack approach and its main purpose is to filter out unwanted traffic. Filtering is implemented by exporting host-routes to each and every router. On Backbone routers, these host-routes are leading to a reject-interface to drop the traffic on a strategic good position.

1.4 Conclusion

The Internet is growing in size and also in importance for the economic market. This makes DoS also an instrument for to influence the market. Common logic or software attacks from the past are fixed. Some of them came back to life with another security patch. Simple DoS attacks like flooding are always possible and there is definitely a trend to DDoS with zombies as attackers. Zombies are hijacked with viruses and trojans spread with hacked web pages of high interest, new Internet technologies and SPAM emails.
The amount and strength of DoS attacks is growing with the Internet, but ISPs have countermeasures available and already in place. Currently without any further and detailed informations from the ISPs it seems that DoS is still a thread but controllable. Reason for this is probably the redundancy of network capacity. How the different defense methods will evolve is hard to tell. The focus for this should be on securing the signaling layers of the defense system. Trust relationship schemes need to be implemented and standardized for such systems. A good link collection to the topic DoS can be found on `http://staff.washington.edu/dittrich/misc/ddos/`

2 SPAM

2.1 Introduction

The term SPAM is said to come from a Monty Python skit from the second series of Monty Python's Flying Circus. In this skit, Vikings sing a chorus about SPAM while a woman tries to get something to eat that doesn't contain SPAM. She tries as hard as she can, but in the end she was unsuccessful in getting a meal that doesn't contain SPAM.
SPAM, one name but many different types. Originally SPAM appeared as a term to describe Excessive Multi Posting (EMP) and Excessive Cross Posting (ECP) on USENET, a worldwide discussion network. Todays most common types of SPAM are probably the Unsolicited Bulk E-mail (UBE) and Unsolicited Commercial E-mail (UCE). Newer types of SPAM are postings in Blogs[1], guestbooks, shoutboxes or picture galleries. These posting contain keywords, hyperlinks and text about products or webpages. Another but more rare type of SPAM are instant messages, which are send out by an automated program. Mostly, these programs just sending thousands of messages on popular instant messaging services but sometimes they are more intelligent and attract a receiver with a common start of a conversation before sending its advertisement. SPAM in Internet Telephony (SPIT) is a recent trend. SPAM in telephony was limited due to the expense involved in making calls, but with free or cheap calls in Voice over IP (VoIP) SPAM in VoIP is on the increase. Just recently[2] there was article about an attack directly on VoIP hardware without the SIP provider in between. Goal of this attack was probably to provoke a callback from the callee.
General goals of SPAM are the distribution of commercial ads, which should attract people to visit websites or inform about products, especially medication. Other goals are spreading malware like trojans and viruses, or so called *fishing* E-mails which fake official E-mails to get credit card information and bank account information. The newer type of SPAM, such as posting comments in all possible types of interactive web pages, are used to manipulate the ranking in search engines. Ranking of an web page is mainly oriented on how many references are pointing to it and by posting comments with these references included this amount is increase. The web page gets more popular from the statistical point of view.

[1] http://en.wikipedia.org/wiki/Blog
[2] http://www.heise.de/newsticker/Erste-groessere-Attacke-gegen-deutsche-VoIP-Nutzer–/meldung/116335

2.2 Distribition of SPAM

For distributing SPAM of any kind, the spammers use automated commercial software or have developed their own specialized software. Examples for such software are for mass sending modified E-mail clients or trojan horse software which is used to create so called "Botnets", which are hijacked computer systems connected by hierarchic or point to point (P2P) networks. During the last two years, there is a trend to P2P networks. This can be explained by the general trend to P2P technology, but the main reason is that P2P networks are more resistant. An hierarchic network can easily be shutdown by cutting of the root node. P2P networks just fall into clusters if important nodes are cut off.
A Botnet can use the hijacked computer systems to harvest E-mail addresses from the user's contact lists and can send massive amounts of SPAM of many different types. Hijacked computer systems[3] are hacked Internet servers and more and more personal computers which were infected by viruses, trojan horses or by exploits for common operating systems and common software like an Internet Browser. Because the SPAM is being sent out by a large number of computers, it's very difficult to track the originator. The originator of the actual SPAM message is a hijacked computer which is just controlled by the spammer, which makes it even harder to track him down. In the past spammers used "Open relays", which are E-Mail servers configured in such a way that it allows anyone on the Internet to send e-mail through it and not just E-mail destined to or originating from known users. By switching default configurations to not allowing relaying, this issue is mostly resolved. For E-mail, the spammers are using web spiders to harvest valid E-mail addresses for potential SPAM victims. Another common way is to guess valid addresses by generating them from dictionary words. These words are mainly common names in the certain country where the SPAM is supposed to be distributed. Accordingly to CNET[4], Europe is still the top source of SPAM for E-mail SPAM.

2.3 Approaches to Reduce the Amount of SPAM

Countermeasures against SPAM can be grouped into three classes. First group is the filtering messages of any kind. This surely includes E-Mail but instant messages, chats, interactive web pages and does not stop with filtering incoming or outgoing telephone calls. Second groups is the verification of a sender before allowing him to send a message. There third group is the simple approach to hide an e.g. E-Mail address as long as possible from the spammers and give it only to trustworthy correspondents or validate that a sender is human and not a computer.
Main focus in this section will be on E-Mail filtering, because for this type of SPAM these

[3] http://computer.howstuffworks.com/zombie-computer2.htm
[4] http://news.cnet.com/Europe-still-top-source-of-SPAM/2100-7349_3-6229352.html

techniques are nearly standard and more sophisticated. Most of the described approaches can be transformed to be used with every other type of SPAM.

2.3.1 Filtering

Latest method of spammers to avoid filters is to use a E-Mail attachment in a format that is not readable or processable by standard filters. This is implemented by rendering the E-Mail text as a picture, use the Portable Document Format (PDF) or compressed archieves like "ZIP". Rendering text as a picture makes the message still readable for humans but very hard to read for a filter. Using other or unknown formats and attach them to the email bypasses the SPAM text and it is not processed by a filter. Some spammers even test their messages with common filters till they pass them before sending the SPAM out. All filtering measures add another step to process a message and slows down the message delivery. Most common filter methods are the following.

- **Checksum based filtering**
  From each message a checksum is generated and compared to a list with known SPAM. Checksum generation is quite fast and keeps processing overhead reasonable. The list of known SPAM needs to be extended or at least validated by a human to avoid non SPAM messages from being filtered out.

- **Statistical content filters**
  Statistical filters create indicators from a message and if a certain threshold is reached, the message is filtered out. Indicators can be for example the amount of words that are often used by SPAM messages in relation to the whole amount of words. A popular example for this type of filters are "naive Bayes classifiers". Statistical filters need more processing than checksum based filters, because they are more complex. The advance of statistical filters is that they can identify new SPAM messages from already known messages. On the other hand the probability of false positives is much higher.

The next three filters are probably the most classical ones. They are very simple but with enhanced or distributed list management very effective compared to processing overhead introduced by them.

- **Blacklisting**
  The source address of a message is compared to a so called blacklist. Every Message is dropped if there is a match with an entry on the blacklist.

- **Whitelisting**
  The source address of a message is compared to a so called whitelist. Every Message that matches with an entry on the whitelist bypassed every further checks or filtering and is directly delivered to the receiver.

- **Greylisting**
  Greylisting is based on a feature from the Simple Mail Transport Protocol (SMTP), which allows a temporary rejection of an incoming message. Although, the message is put into a queue and waits till a SMTP standard conform client tries again. After a certain timeout the message is deleted from the queue. If the client retries before the timeout the server starts the delivery, which could also involve some further filtering. All this is based on the assumption that spammers only try once.

2.3.2 Sender Verification

Sender verification tries to build a trust relationship to the sender using basic authentication or cryptographic measures. This section gives a short overview about common methods for Sender Verification.

- **SMTP Authentication**
  Original SMTP does not define any authentication. Receiving emails e.g. with the Post Office Protocol (POP) is normally secured by basic authentication. The simplest approach of SMPT Authentication is to have the policy "POP before SMTP". During the POP login, the IP address is stored and till a certain timeout this IP address is allowed to send E-Mail via SMTP. More sophisticated is to used RFC 2554[5], which defines a authentication directly for SMTP.

- **ForwardConfirmed Reverse DNS (FCrDNS)**
  ForwardConfirmed Reverse DNS is that a sender IP address can be reversed to a DNS name and matches with the given name of the sender. This creates a weak form of authentication and is mainly used in SMTP servers. Also the existence of a DNS name could be an authentication attribute. On the other hand this type of authentication can be used for whitelisting purposes because spammers can not usually by-pass this verification when they use zombie computers to forge the domains.

- **Certified Messages**
  Asymmetric key Cryptographic and Cryptographic certificates are used for authentication of messages. Strong cryptography is powerful and secure enough to let a authenticated message bypass all further checking or filtering. A Public key infrastructure (PKI) needs to be in place. There are already commercial service providers like "Goodmail Systems"[6]. A pay per message can be implemented.

[5] http://www.ietf.org/rfc/rfc2554.txt
[6] http://www.goodmailsystems.com/

- **DKIM (DomainKeys Identified Mail)**
  This is very similar to the the Certified Messages, but the public keys are exchange via DNS. A PKI is implemented by the hierarchic structure of the DNS. The message body is protected by a hash, usually SHA-256. Message headers and the hash is signed with RSA.

- **HELO or EHELO checks**
  HELO or EHELO is part of SMTP and is used from the client to identify itself by DNS name. Policies for this type of checks could be that a given source domain is checked by reverse lookups (see FCrDNS) or that unresolvable names not allowed to send any message.

2.3.3 Other Methods

Other approaches can be to rate limit the amount of messages a sender is allowed to send in a certain time. This could be worked around by the spammers by slowing down the sending rate, but increasing the amount senders. On interactive web pages a technique called Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA) got very popular. By letting the user type in numbers and/or letters from a hard to read picture which is randomly created for every authentication try, it is assured that the sender is human and not machine. As a response the spammers developed specialized text recognition software, which can read the numbers and letters sometimes better than a human. The needed processing power is available from the hijacked computer systems. More creative is the approach to use pornography to let the for software unreadable CAPTCHAs read out by humans. As described by a Heise article[7], spammer promise to the interested web page visitor to show another pornographic picture if he solves the CAPTCHA.
Finally, there is still the attempt to not public publish an address to avoid SPAM. Addresses are only given to trustworthy correspondents and the address itself needs to be hard to guess. For web pages there is the possibility to use a input formula instead of publish a contact address. To protect an address from being harvested with a software it can be rendered as a picture or dynamically rendered into the page with JavaScript. It can be said that every anti SPAM technique which is used by a large percentage of the users is adopted by the spammers and used for their purposes.

[7] http://www.heise.de/newsticker/Porno-gegen-Captchas–/meldung/113239

2.4 Conclusion

New communication techniques are adopted for spamming and the amount of SPAM is still growing with the Internet. For E-mail the main percentage of messages are SPAM message. SPAM is successful by the huge amount of messages and not by the success rate, although a small success rate is enough for the spammers to have a good life because sending out SPAM is so cheap.
SPAM and DoS has in common that for both thing Botnets are used. No ultimate solution is found (yet) to get rid of SPAM, but it can be heavily reduced by advanced filtering and sender verification.

Bibliography

[Allman] Mark Allman. *A Web Server's View of the Transport Layer.*
http://www.icir.org/mallman/tcp-opt-deployment/
NASA Glenn Research Center/BBN Technologies, October 2000

[CA-1996-21] CERT Advisory. *TCP SYN Flooding and IP Spoofing Attacks.*
http://www.cert.org/advisories/CA-1996-21.html/
Carnegie Mellon University, September 1996

[CA-1996-01] CERT Advisory. *UDP Port Denial-of-Service Attack.*
http://www.cert.org/advisories/CA-1996-01.html
Carnegie Mellon University, September 1997

[CA-1997-28] CERT Advisory. *IP Denial-of-Service Attacks.*
http://www.cert.org/advisories/CA-1997-28.html
Carnegie Mellon University, December 1997

[CA-1998-01] CERT Advisory. *Smurf IP Denial-of-Service Attacks.*
http://www.cert.org/advisories/CA-1998-01.html
Carnegie Mellon University, January 1998

[Czmok] Jan-Ahrent Czmok *Detecting DDOS Attacks and Countermeasures at ISPs*
Chaos Communication Congress, December 2002

[Eckert] Prof. Dr. Claudia Eckert *Distributed Denial of Service - Angriffswerkzeuge und Abwehrmöglichkeiten*
TU Darmstadt, Fall 2002

[Mittner] P. Mittner, I. Schmid, B. Studer *DDOS Attacken*, section 1.4.8
HTW Chur, Fall 2000

[Ruef] Marc Ruef, Marko Rogge, Wolfram Gieseke, Uwe Velten *Hacking intern*, chapter 4
Data Becker, November 2002