Trusted Information Sharing Network
for Critical Infrastructure Protection

Denial of Service / Distributed Denial of Service

MANAGING DoS ATTACKS

June 2006

ISBN 0 642 75362 8

CONTENTS

REFERENCES

Figures

Case Studies

EXECUTIVE SUMMARY

With the advance of information and communication technologies, our societies are evolving into global information societies with a ubiquitous computing environment that has made cyber attacks significantly more sophisticated and threatening [1]. One type of cyber attack that is becoming more prevalent today is that known as a Denial of Service attack.

The Trusted Information Sharing Network (TISN) is an Australian forum in which the owners and operators of critical infrastructure work together by sharing information on security issues which affect critical infrastructure. This document has been developed by the IT Security Expert Advisory Group (ITSEAG), which is part of the Trusted Information Sharing Network (TISN)[2] for critical infrastructure protection.

Information security is generally categorised as the safeguard of confidentiality, integrity and availability of information and information systems. A Denial of Service (DoS) attack is a type of attack focused on disrupting availability. Such an attack can take many shapes, ranging from an attack on the physical IT environment, to the overloading of network connection capacity, or through exploiting application weaknesses.

One hundred per cent availability of systems and networks is widely accepted to be unattainable, regardless of diligence or the amount of resources allocated to securing systems against attack. Internet-facing and other networked infrastructure components are at risk of DoS for two primary reasons.

1. Resources such as bandwidth, processing power, and storage capacities are not unlimited and so DoS attacks target these resources in order to disrupt systems and networks.
2. Internet security is highly interdependent and the weakest link in the chain may be controlled by someone else thus taking away the ability to be self reliant.

Over time, the systems used by providers of Australian critical infrastructure have become increasingly interconnected. As this interdependence has grown, exposure to Denial of Service threats has increased, creating a need for best practice protection strategies in the area.

---

[1] APEC. 2005. APEC Strategy to Ensure Trusted, Secure and Sustainable Online Environment.

[2] TISN enables the owners and operators of critical infrastructure to share information on important issues. It is made up of a number of sector-specific Infrastructure Assurance Advisory Groups (IAAG), several Expert Advisory Groups (EAGs), and the Critical Infrastructure Advisory Council (CIAC - the peak body of TISN that overseas the IAAGs and EAGs). More on TISN can be sought from *www.tisn.gov.au* or by contacting cip@ag.gov.au.

The ITSEAG is one of the EAGs within the TISN framework. The ITSEAG provides advice to the CIAC and the sector-based IAAGs on IT issues as they relate to critical infrastructure protection. It is made up of academic specialists, vendors, consultants and some industry association representatives who are leaders in the information technology/e-security field. The ITSEAG Secretariat can be contacted on 02 6271 1595.

This report examines Denial of Service (DoS)—the broad field of attacks focused on disrupting availability—and Distributed Denial of Service (DDoS)—an attack originating from many sources – as they relate to Australian critical infrastructure and provides guidance for management of DoS threats. As DDoS is effectively a type of Denial of Service attack, throughout this report, references to DoS include DDoS unless stated.

Many motivations exist for DoS attacks. They include financial gain through damaging a competitor's brand or by using extortion, raising one's profile in the hacker community, or even simple boredom. Recently, politically and revenge driven attacks designed to disrupt an organisation's—or indeed a country's—operations have become more prevalent.

The costs of DoS attacks to critical infrastructure organisations can be significant. A respondent to the 2005 Australian Computer Crime and Security Survey reported a single-incident loss of $8 million arising from a DoS attack. For many critical infrastructure companies, a significant and prolonged period of system unavailability could result in losses an order of magnitude higher than this.

In addition to the potential for significant financial loss, the make-up of some critical infrastructure organisations means that the impact of downtime may not be limited to lost revenue and goodwill but will extend to social and human costs through an inability to deliver essential services. In extreme cases, this could indirectly include a loss of life —such as through a DoS impact on the health system, or delays in emergency service dispatch. Other costs may include those suffered due to litigation and contractual violations, stock price fluctuations and even intangibles such as decreased morale and loss of reputation.

To mitigate the risks of DoS and DDoS attacks, a best-practice approach is required that includes an overarching strategy combined with operational and technical measures. Processes, procedures, software and hardware can be put in place that will protect systems prior to attack, detect malicious activity as it occurs and support the organisation in reacting appropriately as required. As a result of the nature of DoS attacks, it is often the case that strong reactive mechanisms are the best form of defence.

Actions that can be taken by organisations in their policies and strategic approach to managing the DoS threat are:

- incorporating DoS into organisational risk management;
- implementing a security management framework;
- undertaking staff training;
- negotiating Service Level Agreements (SLAs) to include DoS response;
- participating in joint exercises;
- improving information sharing; and
- obtaining Insurance.

Protection from DoS attacks poses a challenge because no single technology or operational process will on its own provide sufficient protection. Undertaking a technical risk assessment allows an organisation to distribute resources as required in protective processes such as capacity planning, network and application design and

review, and business continuity planning. Once adequate operational measures are in place, anti-DoS technologies, traffic filtering, system hardening, and other technical mechanisms can be reviewed and deployed.

Given the range of attacks covered by the broad umbrella of 'Denial of Service', it is often not easy to know when an organisation is under attack. In the DoS case, the effects are likely to be immediate and result in a system or subsystem becoming unavailable. The symptoms of a DDoS attack may take longer to appear and are usually apparent in slow access times or service unavailability.

It is for this reason that a strong technical incident detection capability will support the management of DoS threats. While technical measures cannot always be relied upon individually, a combination of the use of intrusion detections systems, logging and monitoring systems, and honey-pots will significantly increase an organisation's ability to accurately detect and identify DoS and DDoS attacks.

The ability to respond promptly and effectively to attack is likely to be of greatest importance to many organisations. 'Reactive' operational processes generally involve incident response and analysis. Actions that can be taken by organisations to improve operational response capability for managing the DoS threat are:

- implementing incident response planning;
- establishing provider relationships;
- performing attack analysis;
- deploying intrusion prevention systems;
- applying rate limiting;
- black-holing malicious traffic;
- using upstream filtering;
- increasing capacity; and
- redirecting domain names.

The following report will guide the reader through the process of preparing for, identifying and reacting to a possible Denial of Service attack. This briefing paper underpins related documents including CEO[3] and CIO[4] guidance papers. The CEO paper contains concise summaries of the critical DoS-related information that is pertinent to CEOs and Directors of Critical Infrastructure organisations. Similarly the CIO paper contains information for CIOs with deeper analysis of operational issues.

BACKGROUND

Many papers and resources exist detailing technical specifications for DoS and DDoS classification, detection, and protection schemes. However, these are extremely focused on a single technical area and do not provide an overall best-practice framework for managing the entire space. Conversely, many standards exist dictating an overall IT or

[3] Trusted Information Sharing Network. 2006. Managing DoS Attacks: Advice for CEOs and Boards of Directors. *www.tisn.gov.au*

[4] Trusted Information Sharing Network. 2006. Managing DoS Attacks: Advice for CIOs. *www.tisn.gov.au*

risk-management approach but are not sufficiently detailed in the area of DoS and DDoS. Furthermore, none of the above relates directly to critical infrastructure. This project and supporting deliverables seek to fill this gap.

The Department of Communications, Information Technology and the Arts (DCITA), on behalf of the IT Security Expert Advisory Group (ITSEAG) of the Trusted Information Sharing Network (TISN), has engaged SIFT to produce a TISN-in-confidence report and supplementary guidance for enterprise-level security for the prevention and management of Denial of Service/Distributed Denial of Service attacks for owners and operators of critical infrastructure.

In developing this body of work, SIFT engaged in discussions with members of the ITSEAG and other relevant bodies including key stakeholders from the IT and information security sectors and owners and operators of critical infrastructure to gain an industry perspective on the issues.

STRUCTURE

This paper is organised into two major sections which can be reviewed independently but are designed to be read sequentially. The first section titled "Threat Assessment" seeks to provide an introduction to the DoS threat to critical infrastructure while the goal of the second is to deliver pragmatic advice on managing the identified risks.

Threat Assessment examines the various DoS risks to critical infrastructure following the AS 4360 Standard for Risk Management. Firstly, the context of DoS is established, then attack vectors are identified, followed by an analysis of risk, and finally the evaluation of those risks. This is illustrated in Figure 1: AS 4360.

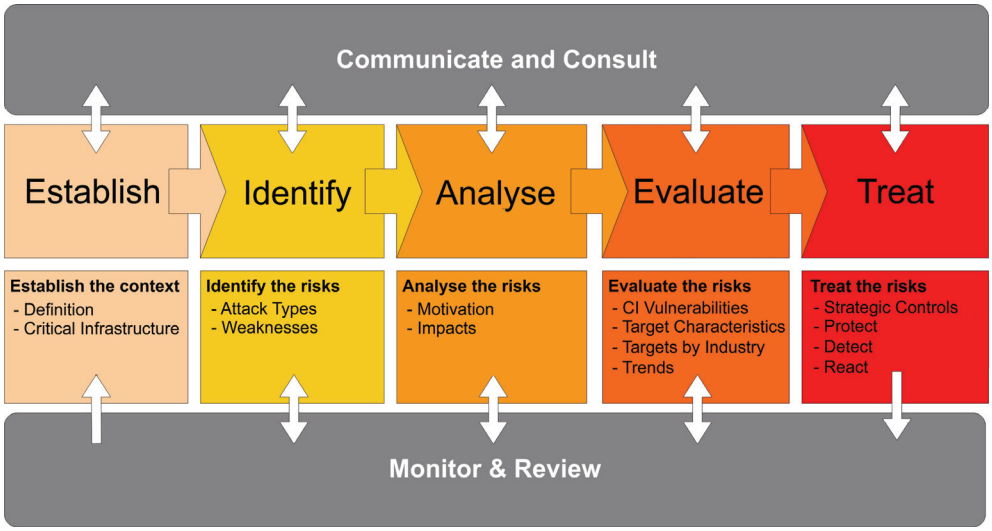

Figure 1: AS 4360 Risk-Management Framework

The framework for DoS management presented provides coverage of security prior to an incident, during an incident and after an incident. This is achieved by detailing a governing strategy and specific recommendations at both operational and technical levels for:

- protecting against DoS and DDoS attacks;
- detecting attacks when they occur; and
- responding appropriately to counter current and future attacks.

It should be noted that while an ‘all threats’ approach to DoS risks is taken in this report, greater emphasis is placed on electronic/network attacks than non-network attacks, and a similar emphasis is placed on those attacks which are considered most likely to occur.

THREAT ASSESSMENT

CONTEXT

Definition

In a Denial of Service attack, the attacker attempts to prevent users or other systems from accessing resources in a timely manner. The Internet Security Glossary[5] defines Denial of Service as "The prevention of authorised access to a system resource or the delaying of system operations and functions."

DoS attacks are often described in terms of two 'types' of attacks—distributed and single-point—which are addressed in the following sections.

Critical Infrastructure

The Attorney-General's Department of the Australian Federal Government has defined critical infrastructure as "Those physical facilities, supply chains, information technologies and communication networks that, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation or affect Australia's ability to conduct national defence and ensure national security."[6]

In this context, the following industries are considered by this paper, with utilities and telecommunications providing the underpinning support services.

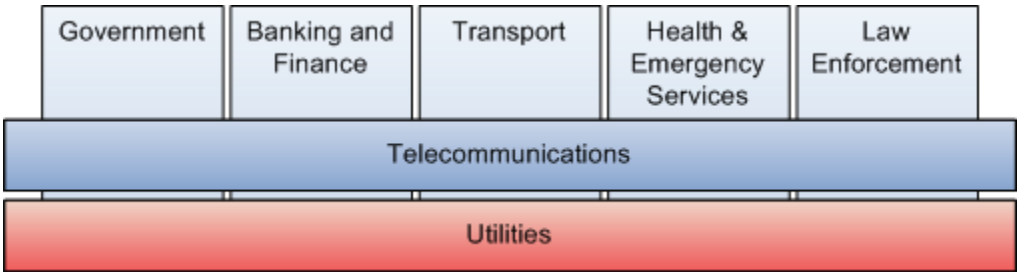

Figure 2: Critical Infrastructure Industries

Critical infrastructure protection is a coordinated blending of existing specialisations, many of which may be affected by DoS. These include:

- law enforcement and crime prevention;
- counter terrorism;
- national security and defence;
- emergency management, including the dissemination of information;

[5] Shirley, R. GTE / BBN Technology. 2000. Internet Security Glossary. *RFC2828.*
[6] Attorney-General's Department. 2006. Trusted Information Sharing Network: About Critical Infrastructure. *www.tisn.gov.au*

- business continuity planning;
- protective security (physical, personnel and procedural);
- e-security;
- natural disaster planning and preparedness;
- risk management;
- professional networking; and
- market regulation, planning and infrastructure development.

RISK IDENTIFICATION

ATTACK TYPES

At first glance DoS attacks appear simple to define and distinguish, but they can be categorised and sorted in numerous overlapping ways. From scale and distribution to target and resource being used, it is apparent that a complete taxonomy is not trivial. The important distinctions are:

- attack vectors;
- singe point vs. distributed;
- client vs. server;
- communication layers;
- attack mechanics; and
- tools.

For those requiring additional detail, a more technical classification is available in *A Taxonomy of DDoS Attack and DDoS Defense Mechanisms*[7].

Attack Vectors

Services that are subject to DoS attacks are not restricted to the electronic medium. Although this report focuses predominantly on electronic communications and systems, DoS can be caused throughout the entire people, processes, and technology paradigm of defence in depth[8].

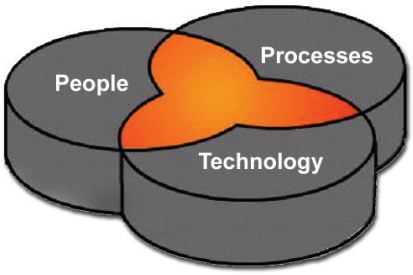

Figure 3: Defence in Depth

People with access to systems can be tricked or 'socially engineered' into shutting them down or changing their configuration. Loopholes in procedures can be abused to force long delays in processing of customer requests. Technology such as mechanical pumps which are operated remotely through an internet device can be sabotaged.

Single Point vs. Distributed

The distinction between a Denial of Service (or single-point DoS) attack and a Distributed Denial of Service attack is the number of originating entities. A single-point DoS has only one source while a Distributed DoS will have many. While single-point

[7] Mirkovic, J and Reiher R. 2004. A Taxonomy of DDoS attack and DDoS Defense Mechanisms. *http://lasr.cs.ucla.edu/DDoS/ucla_tech_report_020018.pdf*
8 NSA. Defense in Depth. *www.nsa.gov/snac/support/defenseindepth.pdf*

DoS threats and countermeasures are well known, Distributed DoS is a newer, less understood form of attack.

A single-point DoS attack will not typically utilise tactics that consume network or other connectivity-related resources because of the difficulty in generating such a volume of data. In general, the aim of this attack is to abuse specific vulnerabilities in business logic or system components to induce a Denial of Service. A common example is the 'ping of death'[9] which was widely used to crash older operating system installations in the late 1990s.

Figure 4: Single-point Denial of Service

A Distributed DoS attack employs multiple disparate attacking entities to execute the attack; however, it is common for the distributed entities to be effectively under the control of a single primary attacker. Rather than attacking a target directly, perhaps with a single high-speed connection, the attacker will instruct a number of previously compromised computers (which individually may only possess slow to moderate connections) to attack the target. The combined power of many scarcely resourced attacking entities creates a significant resource.

A DDoS attack will typically proceed as follows:

1. An attacker will compromise many hundreds or even thousands of machines via automated means, such as a worm, or by manually breaking into each system over a period of time. The compromised machines are known as 'zombies'.
2. Malicious software called a 'bot' (short for robot) will be installed on each compromised machine to allow future remote control of the machines. These are collectively known as a 'botnet' (short for robot network).
3. Once an attacker has control over a sufficiently sized botnet, they will instruct all the zombies to attack the target simultaneously.
4. Due to the vast bandwidth resources available to the botnet, the target system or underlying network will collapse under the sheer volume of connections or data.

To illustrate this scenario:

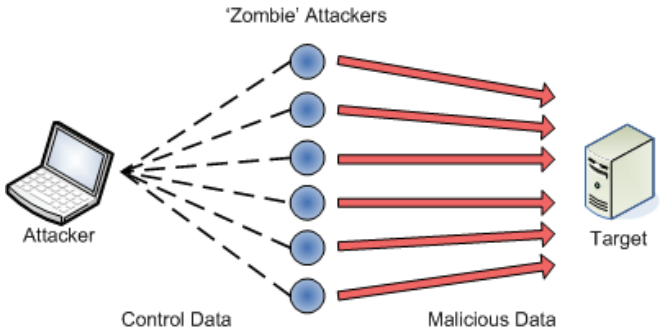

Figure 5: Distributed Denial of Service

[9] Malachi Kenney. 2006. Ping of Death. *www.insecure.org/sploits/ping-o-death.html*

Client vs. Server

Accessing a networked service or functionality at a high level involves two parties. The first, loosely termed the *server*, provides the service to the accessing party, loosely termed the *client*. Although other networking paradigms such as peer-to-peer do exist, any communication still occurs between two high-level parties, each of which is a potential target for attack. The prevention or delay of authorised access to a system resource can therefore be achieved in one of two ways:

1. by impeding the ability of the server to provide the service; or
2. by impeding the client's ability to access the service.

DoS attacks against the server side of the connection are by far the most common because, in general, the attacker intends to affect all users (clients) of a resource rather than a particular subset. Furthermore, it is usually difficult to identify the users of a system and directly target them.

Communication Layers

The ISO Open Systems Interconnection Reference Model[10] divides communications into seven layers as shown in Figure 6: OSI Reference Model, below. Each layer is dedicated to performing a specific function on the data being communicated. The application layer is where the meaningful business logic occurs while the actual data transfer occurs at the physical layer, with intermediate layers translating between data types and facilitating meaningful exchange.

It is therefore possible to target any of these layers in a DoS attack because there is no electronic medium without an attack vector. The lower the layer being attacked, the larger the resource space affected because high layers rely on the services provided by the lower layers. This property is the cause of 'collateral damage' that often occurs to organisations which are not a target of a given DoS attack, but rely on low layer infrastructure shared with the target. Attacks directed at the higher layers of the stack are generally more sophisticated and tend to be harder to detect and prevent.

Examples of attacks on each layer include:

- Application—Corrupting the application database so that no processing of data is possible. Examples of application DoS vulnerabilities include[11], [12], and [13].
- Presentation—Injecting formatting tokens so that information presented is no longer understandable.
- Session—Submitting a logout message using a session identifier that is bound to another user.

---

[10] ISO/IEC. 2000. Basic Reference *Model: The Basic. Open Systems Interconnection*. *www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=20269&ICS1=35&ICS2=100&ICS3=1*

[11] Waldegger, T. 2006. Mozilla Firefox HTML Parsing Null Pointer Dereference Denial of Service Vulnerability. *www.securityfocus.com/bid/17499*

12 Zalewski, M. 2005. Microsoft Internet Explorer JPEG Image Rendering CMP Fencepost Denial of Service Vulnerability. *www.securityfocus.com/bid/14284*

13 Apelt, S. 2005. Veritas Backup Exec Remote Agent Null Pointer Dereference Denial of Service Vulnerability. *www.securityfocus.com/bid/14021*

- Transport—Using a 'SYN flood' to cause the server to allocate vast amounts of resources for connections that will never be completed.
- Network—Using a 'Teardrop' attack which involves sending highly fragmented IP packets to a target, requiring significant resources to reassemble.
- Data Link—Using an 'ARP spoofing' attack to pose as a gateway by supplying a spoofed address, and subsequently refusing to deliver messages.
- Physical—Unplugging of the network cable connected to a server.

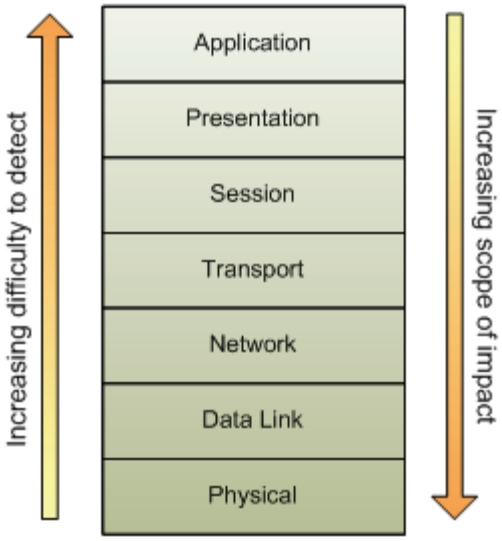

Figure 6: OSI Reference Model

In addition to the above layers, an underlying 'environment' layer is necessary to describe threats posed to physical facilities hosting systems and networks. This is due to the inherent support provided by the physical environment to the networked world. An example threat at this layer is the use of a fire alarm to prevent IT administrators from accessing equipment for a short period.

Attack Mechanics

A popular DoS classification method involves the use of the attack mechanism as the distinguishing factor. That is, for any DoS attack, asking: "What means was used to execute the attack?"

CERT/CC prescribes the following classification[14] of Denial of Service using this approach. It is the most widely used and accepted categorisation.

- Consumption of scarce resources
  - Network connectivity
  - Using your own resources against you
  - Bandwidth consumption

14 CERT/CC. 1999. Denial-of-Service attacks. *www.cert.org/tech_tips/denial_of_service.html*

    - Consumption of other resources
- Destruction or alteration of configuration information
- Physical destruction or alteration of network components

However, since this definition was established the attacks have evolved and this is no longer a full definition as it fails to recognise attacks that do not rely on the consumption or destruction of resources. For the purposes of this paper the following additional category will be added:

- Abuse of business logic

A comprehensive list of known low-level types of Denial of Service attacks under these categories is provided in Appendix B: Known Attacks.

Tools

DoS and DDoS tools are available in a number of flavours, from simple single-target exploits to sophisticated self-propagating DDoS bots which are similar to Internet worms.

DoS vulnerabilities are being discovered regularly in even the most high-profile applications. Almost immediately upon discovery of these vulnerabilities, 'point-and-click' tools are published to exploit them. These tools can often be freely downloaded and used to directly disable vulnerable applications within the space of a single interaction. An example of this is the Microsoft Windows Plug and Play Denial of Service Vulnerability [15].

Originally, Distributed Denial of Service tools such as Trinoo [16] were standalone applications created for the sole purpose of executing attacks. Such tools are no longer as prevalent as they once were.

Today, hybrid approaches in the form of bots are the tools preferred by attackers. Bots contain similar attack functionality to previous generations of tools but they vastly increase the automation of the attack process. Bots such as Agobot [17], can be instructed to automatically spread to other machines, infect additional hosts, upgrade core functions and initiate attacks, all from a centralised control point. Most anti-virus vendors now classify bots as worms (as opposed to attack tools).

A comprehensive list of tools is available in Appendix C: DoS Tools.

WEAKNESSES

Many forms of DoS attacks, especially distributed attacks, are facilitated by fundamental weaknesses in today's computing infrastructures. Some issues include:

- insecure systems;
- lack of authentication;

---

[15] SecurityFocus. 2005. Microsoft Windows Plug and Play Denial of Service Vulnerability. *www.securityfocus.com/bid/15460/exploit*
16 David Dittrich. 1999. The DoS Project's 'Trinoo' distributed Denial of Service attack tool. *http://staff.washington.edu/dittrich/misc/trinoo.analysis*
17 infectionvectors.com. 2004. Agobot and the "Kit"chen Sink. *www.infectionvectors.com/vectors/Agobot_&_the_Kit-chen_Sink.pdf*

- existence of reflectors and amplifiers; and
- problematic attack identification.

Additionally, some secondary weaknesses and causes exist.

Insecure Systems

The SANS Internet Storm Center[18] reports that the current survival time for an unpatched Windows machine before it is compromised is 78 minutes. A graph of survival times of different systems is shown in Figure 7: Pre-infection Survival Time, below. The majority of DDoS attacks rely on the abundance of insecure systems which can be controlled and attached to vast botnets.

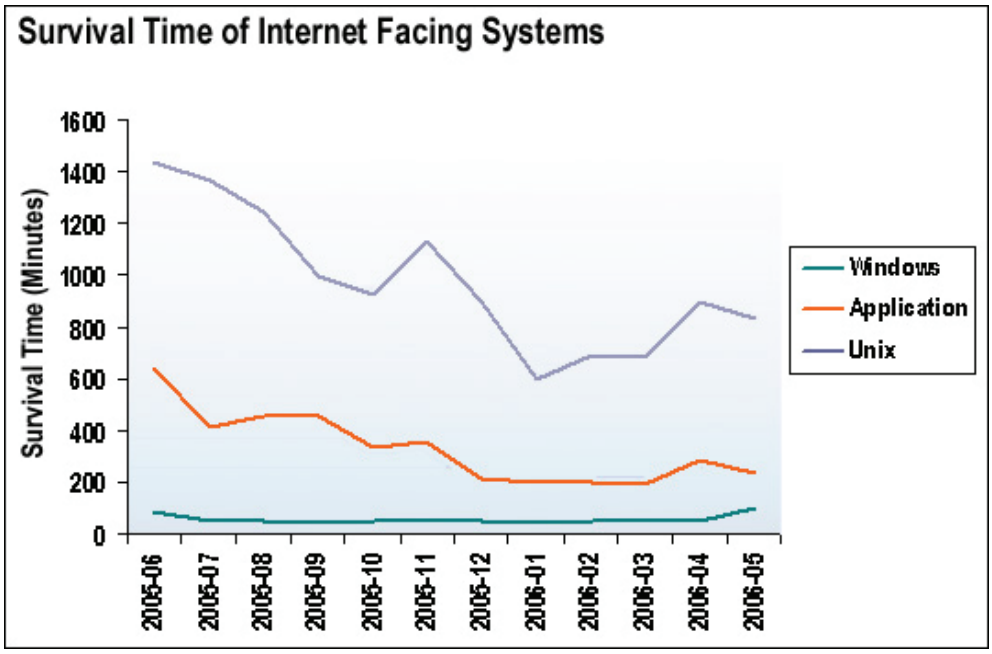

Figure 7: Pre-infection Survival Time

This low survival time is directly related to weak patching processes and the increased speed at which attackers are developing and deploying exploits to released vulnerabilities. Given this, organisations face diminishing timeframes in which patching is effective in countering exploits. It is now not uncommon to see mass exploitation of vulnerabilities within days of vulnerability publication, and in some cases even prior to public disclosure and patch availability.

Lack of Authentication

Source IP address spoofing is a technique that allows the origin of network messages to be faked. It provides a means of maintaining anonymity and therefore avoiding accountability for those who perpetrate attacks. Furthermore, many reflection and amplification attacks rely on spoofing to direct responses at the target. Spoofing is a direct result of a fundamental lack of authentication in the protocols being used on the Internet.

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

Spoofing also makes it difficult to narrow the scope of defensive measures because the source addresses of malicious traffic may coincide with those of legitimate users and networks.

Existence of Reflectors and Amplifiers

DDoS attack intensity is not always restricted by the number of bots or the total bandwidth available to the botnet. The Internet provides a vast array of 'amplifiers' which can increase the magnitude of traffic generated. This is achieved by either causing larger responses than requests (size amplification) or by causing a larger number of responses than requests (quantity amplification). By default, all systems are 'reflectors' in that they can induced to generate a response to a message, and to send that response to an arbitrary recipient. Amplification is facilitated by this ability to reflect traffic. In some special cases, the reflected traffic is of greater volume than the original requests.

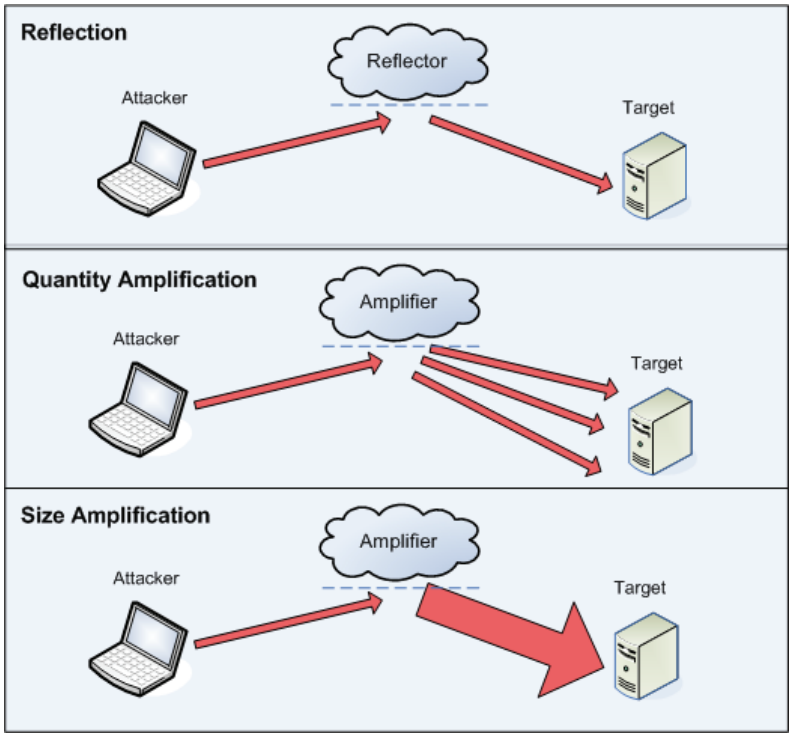

Figure 8: Reflection and Amplification

Some common amplifiers (which are also reflectors) include:

- misconfigured DNS servers;
- networks and hosts which respond to broadcast addresses; and
- network components which fragment packets.

Case Study : Top Level Domain Servers

What happened?

Early February 2006 saw Top Level Domain (TLD) servers come under a series of severe DDoS attacks. The Chief Security Officer of Verisign, host of some of the relevant servers, stated that "These attacks have been significantly larger than anything we've seen." In fact, a post-mortem investigation found that attack traffic was between 1 Gigabit and 2.4 Gigabits per second throughout the attacks.

The perpetrators were able to generate such large volumes of traffic because of many misconfigured servers allowing DNS queries to be amplified towards the target. The vulnerable DNS servers allowed recursive lookups which caused large entries generated by the attackers to be cached. A botnet was then used to query those servers for the supplied large entries which were then sent towards the TLD servers being targeted.

Research suggests that approximately 75 per cent DNS servers are vulnerable to being used as an amplifier.

What was the impact?

Monitoring of DNS servers throughout the attacks showed that up to four servers were unresponsive and noticeable delays could be seen by some users.

How was the situation handled?

The attacks were mitigated by a number of factors including technical analysis and the implementation of identified countermeasures. The DNS network is designed to be distributed and fully redundant such that many of the TLD servers must be unusable for the impact to be significant globally. The malicious messages originated from a set of vulnerable servers and were found to be much larger than typical DNS messages and thus could be filtered at the edge of the networks hosting the servers.

Further information:

www.icann.org/committees/security/dns-DDoS-advisory-31mar06.pdf

http://news.com.com/New+denial-of-service+threat+emerges/2100-7349_3-6050688.html

www.it-observer.com/articles/1120/DDoS_attacks_gear_up_with_ten_times_greater_power/

www.us-cert.gov/reading_room/DNS-recursion121605.pdf

Case Study 1: Top Level Domain Servers

Problematic Attack Identification

A fundamental challenge posed by many DoS attacks is that they exactly simulate and/or mimic normal user activity. That is, any single malicious message is indistinguishable from a legitimate message.

The problem is analogous to what is known as the 'Slashdot effect' [19], coined by users of an extremely popular website which allows users to post news stories with relevant

[19] Wikipedia. 2006. Slashdot Effect. *http://en.wikipedia.org/wiki/SlashDot_Effect*

links. Because of the site's enormous user base, the linked websites often become inaccessible through complete saturation of available bandwidth by legitimate users.

Secondary Weaknesses and Causes

Additional items which are likely to increase the success probability of DoS/DDoS attacks, and which are under the control of the target, include:

- poor planning;
- inadequate provider relationships and contracts with telecommunications providers or Internet service providers;
- insufficient bandwidth capacity;
- lack of testing; and
- poor application design and programming.

RISK ANALYSIS

MOTIVATION

DoS attacks began to occur when a critical mass of organisations and individuals became Internet connected, giving attackers real incentive to strike. "Computer criminals are driven by time-honoured motivations, the most obvious of which are greed, lust, power, revenge, adventure and the desire to taste 'forbidden fruit'."[20] An investigation of available news reports on high-profile incidents indicates that these groups (as they relate to Denial of Service) can be further categorised in the following order of prevalence:

- **Group 1: Monetary gain**

  There are a number of ways attackers can increase their wealth through DoS, most notably via extortion, whereby an initial attack is quickly followed by demands of payment and threats of additional attacks. A number of incidents have demonstrated that DoS is being used as a tool for disrupting competitor operations, thereby poaching dissatisfied customers. It is also not inconceivable that extended periods of unavailability may cause stock price fluctuations.
- **Group 2: Self-actualisation and boredom**

  This motivation includes both the raising of standing (or 'street cred') with peers and the actualisation of one's goals by overpowering or controlling high-profile targets. This motivation is most common to low-skilled attackers (or 'script kiddies') with an excess of time and can often be the result of simple boredom.
- **Group 3: Revenge**

  DoS can be carried out as a retaliation tactic for an injustice perceived by an attacker. This is also generally the domain of low-skilled attackers.
- **Group 4: Information warfare**

  This refers to attacks that are carried out for political reasons, including terrorism and online protests (or 'hactivism') which are typically directed at government and other critical infrastructure organisations.

[20] Peter Grabosky. 2000. Cyber crime and information warfare. *www.aic.gov.au/conferences/transnational/grabosky.pdf*

Case Study : World Trade Organisation

What happened?

In late 1999 the World Trade Organisation website was slowed to a snail's pace in what was one of the first known instances of online protest. The attack carried out during a Seattle WTO conference involved more than 10 000 individuals coordinated by the Electrohippies organisation protesting against various globalisation issues.

The attack was achieved by creating a central page which caused protesters to repeatedly artificially visit the WTO's site which was broadcasting the meeting.

What was the impact?

According to the protest organisers "The WTO's main server was unavailable for periods on Tuesday (November 30)," and the conference server was "intermittently very slow (as compared to our measurements the previous week)."

How was the situation handled?

This case illustrates the problematic nature of DDoS attacks. Each user requested information from a web server through a limited home connection in a manner identical to a legitimate visitor. A single user alone did not disrupt the service; however, as a large group the protesters caused a significant impact. Furthermore, it was difficult to determine which requests were illegitimate as the attackers performed actions no different from regular users.

Further information:

http://news.zdnet.co.uk/internet/0,39020369,2075527,00.htm

http://cyber.law.harvard.edu/studygroup/cybercrime.html

http://archives.cnn.com/2001/TECH/internet/06/20/hacker.vigilantes.idg/index.html?related

www.2600.com/news/1201-fbi.txt

http://news.zdnet.com/2100-9595_22-516972.html

www.fraw.org.uk/ehippies/action/wto_press.shtml

www.fraw.org.uk/ehippies/action/wto_i-review.shtml

Case Study 2: World Trade Organisation

IMPACTS

The impacts of DoS attacks can be many and varied. Attacks can have immense direct financial consequences but typically the intangible ramifications outweigh the monetary. Furthermore, if an attack on a critical infrastructure service is successful, significant 'real world' damage could arise.

The 2005 Australian Computer Crime and Security Survey[21] found that:

> "Only 14 per cent [of respondent companies] reported experiencing Denial of Service (DoS) attacks which resulted in financial loss but overall these losses accounted for about 53 per cent of total losses reported by survey respondents (nearly $9 million). However, during the survey period, one organisation reported losses due to DoS attacks of $8 million. If this figure is excluded, more typical average losses due to DoS attacks were around $70 000."

[21] AusCERT. 2005. Australian Computer Crime & Security Survey.

This illustrates that despite the limited likelihood of DoS, a single occurrence may have catastrophic consequences. Furthermore, many DoS incidents are never reported nor their impact qualified as direct financial loss.

Unfortunately, data on DoS attacks which indirectly impact organisations relying on shared infrastructure is unavailable. For example, many organisations suffer the consequences of spam emails which cause immense volumes of DNS traffic, impacting DNS servers which are used by many customers of ISPs. Furthermore, data on firms that have acceded to the demands of extortionists is also scarce and may encourage further criminal activity.

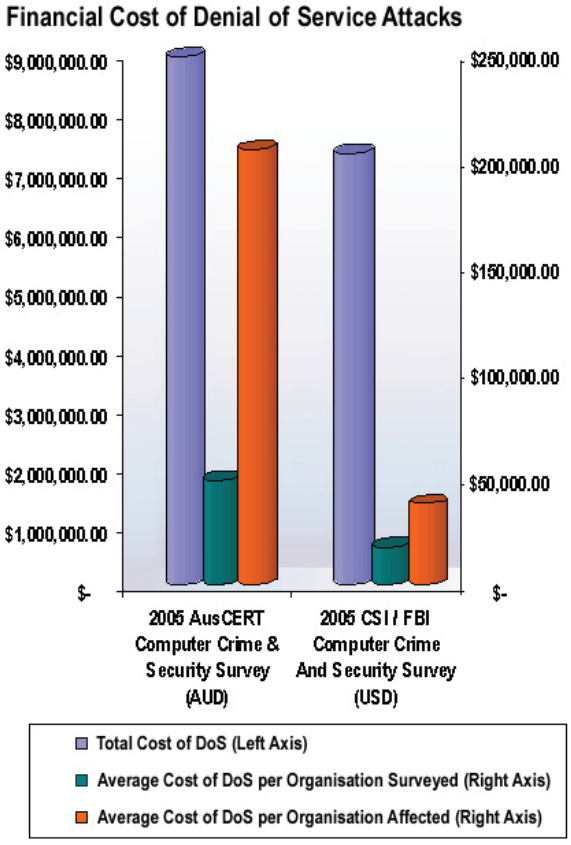

Figure 9: Financial Costs

Financial Costs

The potential financial costs of a disaster similar to a successful DoS attack may already be documented as part of a business impact analysis. The most common financial costs of DoS are:

- **Lost revenue**

  If online functionality is for generating revenue, the ability to generate that revenue will be lost during system unavailability. As outage time increases linearly, it is likely that lost revenue will increase exponentially due to the increasing customer base (including business partners) that is affected.

- **Contractual violations**

  Disruptions in service often hamper the ability of organisations to meet Service Level Agreements (SLAs) which often carry monetary penalties.

- **Litigation costs**

  There are various situations under which the target of attack may face litigation, including failing to provide a service or causing damage to a third party.

- **Service provider expenses**

  Communications service providers are likely to be engaged in detection, reaction, and analysis of DoS attacks and may charge the client organisation for these additional services. Excess bandwidth usage is the responsibility of the subscriber.

- **Incident handling and recovery costs**

  As the target organisation recovers from an incident, human resources must be employed to analyse the attack and restore services. Costs are incurred in the redirection of these resources from their normal tasks.

- **Stock price fluctuations**

  In the event business critical services are interrupted for substantial periods of time, the business impact may produce investor uncertainty.

Intangible Consequences

Intangible costs of DoS often do not receive as much attention when conducting risk analysis. However, the below list demonstrates such costs are an integral part of the full impacts of such an attack.

- **Third-party damage**

  As discussed above, if an attack is targeted at one organisation it may impact others through shared infrastructure. Insecure machines in an organisation's network also may be used to attack other organisations.

- **Morale**

  Employees are motivated when they are able to work efficiently and without interruption. Continual outages may become a burden to those who feel they are unable to complete assigned tasks.

- **Lost productivity**

  If critical systems are inaccessible valuable time may be lost in completing work-related assignments.

- **Brand damage**

  Today's information economy relies on the ability to access resources on demand. Downtime can therefore have long-term impacts, particularly on those organisations which provide public services, gain competitive advantage through reliability, or where customer loyalty is easily swayed.

- **Human costs**

  Included among critical infrastructure organisations are law enforcement, health and emergency services. Any disruption to these services may result in injury or loss of life.

- **E-commerce credibility**

  Prolonged and sustained attacks against critical infrastructure entities and organisations with a high-visibility presence on the Internet may degrade consumer confidence in e-commerce. Damage to the credibility of these systems may have an economy-wide impact.

RISK EVALUATION

CRITICAL INFRASTRUCTURE VULNERABILITIES

In a 1998 white paper[22] and later in Critical Information Infrastructure Protection (CIIP) surveys[23] [24], researchers identified some elements of Australia's infrastructure that could result in severe impact in the event of an electronic or physical DoS attack. Many of these issues have been addressed but undoubtedly some remain and should be analysed in the context of the current interconnected environment.

TARGETS BY CHARACTERISTICS

Some critical infrastructure targets are considered more likely than others to suffer a DoS attack because of their attack profile. In general, the following properties are likely to make a system or organisation more vulnerable:

- the system is Internet-facing;
- the system has one or more single points of failure;
- the organisation or the system are highly visible or have a high media profile;
- the system is critical to the operations of the organisation; and
- the system is highly accessible providing greater opportunity for an attacker.

It is noted that many of the specific systems and targets discussed by Industry, below, would require the involvement of an insider to either provide the necessary information or bypass external controls. The above characteristics can be useful in appraising the relative likelihood of a given system being subject to attack.

TARGETS BY INDUSTRY

Because of the motivations of attackers and the resources being supported by different industries, threat profiles of critical infrastructure organisations will be influenced by the industry in which they operate. The following provides an indication of the systems that could be subject to DoS attack, within each key industry segment.

- **Utilities**

  Utilities provide the fundamental supporting infrastructure for all other organisations. While utilities are less susceptible to common forms of DoS and DDoS because of the use of closed networks and proprietary systems, they are at greater risk of a high-impact event. If a physical or otherwise non-network Denial of

[22] Cobb, A. 1998. Thinking about the Unthinkable: Australian Vulnerabilities to High-Tech Risks *www.aph.gov.au/library/pubs/rp/1997-98/98rp18.htm*
[23] Swiss Federal Institute of Technology. 2004. International CIIP Handbook 2004
[24] Swiss Federal Institute of Technology. 2006. International CIIP Handbook 2006

Service attack occurs, restricting access to a fundamental service such as water or energy, it could adversely impact human and organisational health.

Potential targets include:

- utility management buildings and facilities (e.g. physical damage to a substation);
- billing systems; and
- supervisory Control and Data Acquisitions (SCADA) systems.

- **Telecommunications**

  Telecommunications carriers may not only be the target of Denial of Service attacks but also the transport mechanisms for such attacks. That is, an attack on resources supplied by a carrier to another organisation may inadvertently or deliberately affect the carrier itself. Given that providing access and bandwidth is the business of telecommunications suppliers, such organisations are a likely target for extortion. A DoS which disrupts the service of a large carrier may cause significant damage to countless organisations. All motivations apply equally to this industry.

  Potential targets include:

  - top-level domain servers and ISP domain name servers;
  - carriers;
  - PBX systems;
  - corporate email servers;
  - core routers (public and private);
  - intercontinental communication links;
  - billing systems; and
  - Internet service providers.

- **Government**

  Government systems may be subject to DoS attack for a wide variety of political reasons. Various government bodies provide social and national defence services. Note also that sections below in Health and Emergency and Law Enforcement also include a large number of government entities/systems.

  Potential targets include:

  - welfare distribution and management systems;
  - electoral kiosks;
  - defence systems;
  - E-Tax;
  - E-BAS; and
  - council transaction systems.

- **Banking & Finance**

  Given that monetary gain is a prime DoS motivator, banking and finance organisations are likely targets. They would be severely affected and open to extortion in the event of online services being unavailable for an extended period.

  Potential targets include:

  - clearing systems;

- online banking; and
- trading systems (both retail and institutional).

- **Transportation**

  Many public transportation systems are not sensitive to system-wide DoS attacks but rather are sensitive at single points, such as traffic controller systems. However, commercial transportation systems are more likely to be at risk because of the time-sensitive services they provide, with a large number of transactions occurring close to the time of transport. Additionally, with increased safety and security check requirements, many processes cannot be easily completed offline.

  Potential targets include:

  - airline ticketing systems;
  - mass Transport Movement Systems (most likely by insiders);
  - train signalling systems;
  - security checking processes (e.g. by creating false alarms);
  - shipping inventory and queuing systems; and
  - customs support systems.

- **Health & Emergency Services**

  While typical motivations behind DoS attacks suggest health and emergency services are an unlikely target in peacetime, such organisations may have an increased threat level from terrorism or in times of war. A catastrophic event may occur if the communications or database systems of health and emergency services become ineffective.

  Potential targets include:

  - 000 emergency reporting systems;
  - patient record databases;
  - specialist medial support systems (e.g. hospital wireless networks); and
  - dispatch processes (e.g. prank phone calls).

- **Law Enforcement**

  Attacks on law enforcement are motivated by the two least—common motivations—revenge and information warfare. Attacks on law enforcement may also be carried out to conceal other DoS attacks or unrelated criminal activities.

  Potential targets include:

  - criminal databases; and
  - law enforcement communication networks.

Case Study : White House

What happened?

In early May 2001, Chinese hackers threatened and subsequently carried out DDoS attacks against the official White House website. The motive for the attacks was clearly political, striking on Chinese Labour Day, Youth Day on 4 May, and also in remembrance of the US bombing of the Chinese embassy in Belgrade.

What was the impact?

The first attack rendered the site inaccessible for three hours; the second caused only a brief outage while the third resulted in six hours of downtime. Although the attack was quite small, it nonetheless caused a public relations setback and raised concerns for the resilience of the infrastructure.

How was the situation handled?

The attacks took the form of an unsophisticated DDoS known as an ICMP flood which uses network management messages to saturate the link between a target and its ISP. The attacking nodes were blocked and high-bandwidth servers that were acting as zombies were shut down.

Further information:

http://news.com.com/2100-1001-257068.html

http://archives.cnn.com/2001/TECH/internet/05/08/DoS.warning.idg/index.html

http://news.bbc.co.uk/1/hi/world/americas/1313753.stm

www.computeruser.com/news/01/05/25/news3.html

www.findarticles.com/p/articles/mi_m0NEW/is_2001_May_23/ai_74988164

Case Study 3: White House

TRENDS

DoS attacks have been occurring for several years. As their prevalence and sophistication have increased the issue has become broader and a number of trends have developed. It is forecast that further trends will develop following the path of similar technologies.

Current

- **Reflection and amplification**

  Although reflection and amplification are well-known DoS facilitators, recent incidents [25] suggest their use is once again receiving significant attention.

- **Autonomous propagation**

  DoS tools are now self-propagating and have even used openings left by Internet worms to take control of infected computers. The rate and means by which DoS bots spread continue to increase. Automated propagation has become the primary approach for serious attackers.

[25] ICANN Security and Stability Advisory Committee. 2006. DNS Distributed Denial of Service (DDoS) Attacks. *SSAC Advisory SAC008*. *www.icann.org/committees/security/dns-ddos-advisory-31mar06.pdf*

- **Larger botnets**

  As a result of increased automation and the ever-growing user presence on the Internet, botnet technology has evolved to support extremely large networks. Researchers at the Honey-net Project report [26] they have witnessed botnets of "up to 50 000 hosts". In a recent criminal trial in the United States, prosecutors claimed that a group "ran a zombie network of 100 000 infected computers"[27].

- **Botnet markets**

  Botnets are now an in-demand criminal tool around which an underground commercial market has been established. Botnets are being sold to the highest bidder and even rental agreements have been observed.

- **Organised crime**

  Organised crime syndicates are increasingly[28] targeting corporations in order to disrupt operations and extort money or gain a competitive advantage in a particular market. This trend is not restricted to online gambling firms, as is sometimes speculated, and is quite often successful because of the small payment demanded relative to the cost of significant downtime.

Case Study: Online Gambling

What happened?

BetCris.com is one of many online wagering sites hosted in Costa Rica. Significant downtime is likely to cause customers to quickly move to a competitor. On November 23, 2003, the site received an email with the demand: "You can send us $40K by Western Union [and] your site will be protected not just this weekend but for the next 12 months… If you choose not to pay...you will be under attack each weekend for the next 20 weeks, or until you close your doors."

After amending their network with an off-the-shelf anti-DoS device, BetCris took no further action on the threat. The following weekend BetCris was attacked, crashing the site, its ISP and its provider's network.

What was the impact?

The company lost $1.16 every second or as much as $100 000 per day. The final financial cost was well over $1 million in lost revenue in addition to hardware and labour costs. Furthermore, many customers had taken their business to other gambling sites.

How was the situation handled?

After negotiations with the extortionist, contact with the National Hi-Tech Crime Unit (NHTCU) and consultation with the ISP, all to no avail, BetCris created a proxy architecture to stop malicious traffic at a new ISP with extremely large bandwidth.

[26] The Honeynet Project & Research Alliance. 2005. Know Your Enemy: Tracking Botnets *www.honeynet.org/papers/bots/*

[27] Sophos. 2005. Suspected zombie kings who ran botnet of 100,00 PCs arrested, reports Sophos *www.sophos.com/pressoffice/news/articles/2005/10/va_dutchbotarrests.html*

[28] Papparlardo, D. and Messmer, E. 2005. Extortion via DDoS on the Rise. Network World *www.networkworld.com/news/2005/051605-DDoS-extortion.html*

After two more weeks of sustained attacks and architecture tweaking, the attacks ceased. The business had lost more than $1 million in revenue and plenty more in goodwill and IT infrastructure, but at least the site was now safe from future attacks and the organisation did not capitulate to the extortionist.

Further information:

www.csoonline.com/read/050105/extortion.html

Case Study 4: Online Gambling

Future

- **Attacks on emerging technologies**

  As new technologies such as Voice over Internet Protocol (VoIP) and wireless networking become commonplace, so too will attacks against them. With respect to these technologies, it is noted that significant work has been completed in previous TISN projects looking at the security implications (including DoS) of VoIP [29] and wireless networking [30]. DoS attacks against such emerging technologies are not often considered until the products are well established and other threats have been addressed. A number of application-level DoS attacks have already been identified for high-profile VoIP products.

- **Application layer**

  Attacks exploiting traditional vulnerabilities are constantly moving up the network protocol stack towards the application layer, as lower layers become more secure through common devices such as firewalls. The same trend is likely to occur in the DoS domain as purpose-built protective devices mature and are widely adopted.

- **Peer-to-peer botnets**

  In general bot networks are controlled through a centralised entity such as an Internet Relay Chat (IRC) server. However, this infrastructure is highly susceptible to being commandeered by rival attackers and is easily shut down by law enforcement. Given the trend towards peer-to-peer communications in legitimate networking, a similar shift may occur in DoS technology which, with the aid of cryptography, may enhance resilience to the above issues and render botnets stealthier than before.

- **Realistic behaviour**

  Many protective mechanisms available in the market place differentiate between malicious traffic and legitimate traffic by performing behavioural analysis on communications flow. This is because determining the legitimacy of a single message is difficult, if not impossible. DoS attack tools will likely counter this by simulating realistic actions and traffic patterns to avoid detection.

- **Attacks against anti-DoS infrastructure**

  As can be observed with technologies such as Intrusion Detection Systems (IDS), if security measures and the devices that implement them become highly effective, they themselves become a target of attack [31].

- **Attacks against SCADA systems**

[29] ITSEAG. 2005. Security of Voice over Internet Protocol
[30] ITSEAG. 2005. Wireless Security
[31] Steve Martin. 2001. Anti-IDS Tools and Tactics. *www.sans.org/rr/whitepapers/detection/339.php*

The 2005 TISN paper "SCADA Security—Advice for CEOs,"[32] providing security guidance to owners and operators of Supervisory Control and Data Acquisition (SCADA) systems found that:

- Increasing reliance on public telecommunications networks to link previously separate SCADA systems is making them more accessible to electronic attacks.
- Increasing use of published open standards and protocols, in particular Internet technologies, exposes SCADA systems to Internet vulnerabilities.
- The interconnection of SCADA systems to corporate networks may make them accessible to undesirable entities.

These trends are consistent with the properties identified in this report as making systems more susceptible to DoS attack, in particular the reliance on underlying telecommunications infrastructures and interconnection of systems.

[32] Attorney-Generals Department. 2005. SCADA Security—Advice for CEOs. *Trusted Information Sharing Network*

THREAT MANAGEMENT

OVERVIEW

Perfect availability, like perfect security, is impossible to achieve. Given this, the objective of DoS management should be to introduce appropriate protection measures and to minimise the effects and subsequent costs of a DoS attack, through prudent controls and swift action.

It is recommended management focus on what is important to the business or organisation rather than attempting to protect all systems from all DoS threats. An asset register and business impact analysis is a valuable exercise and an initial step to enable effort and spending to be prioritised.

The justification for DoS defence spending is often a relatively simple Return on Security Investment (ROSI) calculation—given various consequences and their associated likelihood, the average cost per year can be determined. This can also be thought of as the potential 'Cost If No Investment' (CINI).

The justification of spending becomes difficult when analysing defences which have global or societal benefits as opposed to those which benefit a single organisation directly. Local spending is required to protect an organisation from DoS and DDoS, but economy-wide expenditure is needed to protect all organisations from the insecurities of individual systems especially given the interdependencies within critical infrastructure.

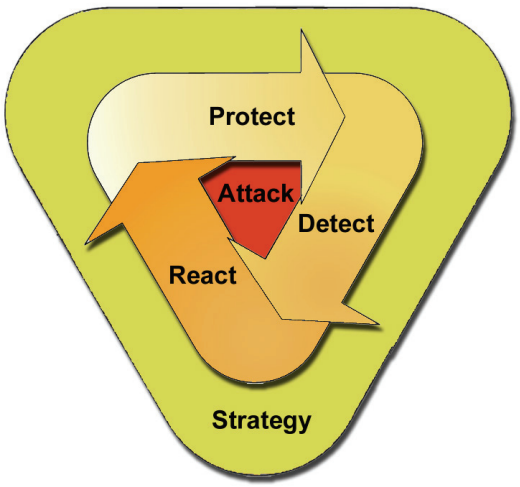

Figure 10: Strategy, Protect, Detect, React

In managing the various DoS risks, critical infrastructure organisations face several challenges:

- Outsourcing is prevalent and as a result an organisation is rarely directly in control of its own infrastructure. Therefore protective capabilities must be funnelled through and agreed with an external party.

- The interconnectedness of various networks and dependency on underpinning infrastructures such as power mean a single organisation cannot implement a unilateral strategy to provide full protection from DoS.
- The fact that a flood-based DoS attack can exactly mimic or simulate normal user behaviour results in a vulnerability which can only fundamentally be treated by adding additional capacity.

The various approaches to DoS management reviewed below are tabulated in Appendix D: Summary of Management Practices.

The recommended approach to managing DoS is to adopt overall strategies, employ protective measures, develop detection procedures, and react appropriately and swiftly.

EXISTING FRAMEWORKS

At the time of writing, there exists only a single dedicated framework for DoS management, providing coverage across all stages of the DoS lifecycle. However, various broader security architectures and targeted standards are applicable to the space and are also presented below.

Managing the Threat of DoS Attacks

Produced in 2001 by the CERT/CC, this [33] is the foremost best-practice framework for managing DoS risks. It is structured around the Protect, Detect, and React triad, providing practical advice for all stages of the DoS lifecycle.

Many of the management practices provided herein are detailed further in this document.

Consensus Roadmap for Defeating DDoS Attacks

This roadmap [34] was developed as part of A Project of the Partnership for Critical Infrastructure Security in the United States. Although the paper was written in 2000, the problems described remain valid and the suggested remediation measures are yet to be implemented on a large scale.

A number of the previously mentioned root causes of DoS are presented along with various potential solutions. Although many of the solutions are applicable at an organisational level, a number prescribe global approaches which if adopted would substantially reduce communal risk.

ISO 17799 Code of Practise for Information Security Management

A comprehensive strategy for protection is the ISO 17799: Code of Practise for Information Security Management [35]. It outlines best practices for organisational protection of information resources. Aligning practices with these requirements will aid

[33] CERT/CC. 2001. Managing the Threat of Denial of Service Attacks. *www.cert.org/archive/pdf/Managing_DoS.pdf*
[34] SANS. 2000. Consensus Roadmap for Defeating Distributed Denial of Service Attacks. *www.sans.org/dosstep/roadmap.php*
[35] ISO. 2005. ISO 17799: Code of Practice for Information Security Management

in the overall management of DoS threats. The following sections are of particular relevance:

- Asset Management;
- Communications and Operations Management;
- Access Control;
- Information Security Incident Management; and
- Business Continuity Management.

ACSI 33 Australian Government Information and Communications Technology Security Manual

In conjunction with the Protective Security Manual, ACSI 33 provides a set of policies and standards to enable Australian Government agencies to achieve a defined level of IT security assurance. The security measures defined in this standard will significantly reduce the likelihood of a Government organisation being successfully targeted by, or participating in, a DoS or DDoS attack. The following sections are of particular relevance:

- Software Security;
- Logical Access Control;
- Communications Security; and
- Network Security.

STRATEGIC CONTROLS AND RESPONSES

A number of actions can be taken by organisations in their policies and strategic approach to managing the DoS threat. Many of the strategic recommendations mentioned herein will fit within the broader IT security governance framework under development as part of the DCITA "Best practice, management and governance for IT and information security guidelines for corporate and business" project. At a strategic level, these will inherently cover the triad of Protect, Detect, and React and include the following:

- incorporating DoS into organisational risk management;
- implementing a security management framework;
- undertaking staff training;
- negotiating service level agreements;
- participating in joint exercises;
- improving information sharing;
- obtaining insurance; and
- introducing industry/government incentives.

Include DoS in Organisational Risk Management

Recent reforms to corporate governance regulations place increased accountability on senior management to manage risks within their organisations. As DoS attacks can have severe consequences for critical infrastructure organisations and their ability to service customers, an organisational risk-management strategy becomes a critical corporate

governance requirement. A structured framework for management of risk, such as AS/NZ 4360, can be applied to DoS to derive greater efficiency in dealing with potential threats.

A number of the interviewed stakeholders stressed that Denial of Service is fundamentally a risk-management issue.

Implement a Security Management Framework

Implementing a security management framework such as ISO 17799 [see 35] provides a holistic view of organisational security risks. Consequently, organisations can develop operational and technical mechanisms to manage these risks. A successful security management framework should aim to create a culture of security, not only implementing and managing technology to combat DoS threats, but also carrying out education and training of staff on DoS and DDoS-related procedures in order to increase vigilance and reduce response time.

Undertake Staff Training

Given the lack of understanding of DoS at a strategic level throughout Australian organisations, it is unlikely that these issues will be well managed at operational and technical levels. It is therefore recommended that organisations consider their exposure to DoS threats and, where relevant, provide adequate training for all levels of staff who may be involved in a DoS incident.

Training should include:

- DoS strategy as a part of security and risk-management strategy;
- implementation and management of anti-DoS technology;
- disaster recovery/incident response procedures;
- DoS detection and escalation;
- communications and reporting procedures; and
- technical analysis of DoS attacks.

Negotiate Service Level Agreements

The nature of Internet infrastructure is such that there is a strong dependency and inter-reliance on various components. For example, users rely on telecommunications providers to access Internet service providers, who in turn rely on root DNS services, who themselves rely on individual registrars, and so on.

A number of functions are typically outsourced by critical infrastructure organisations and are therefore bound by Service Level Agreements (SLAs). Traditional SLAs often do not contain clauses relating to DoS scenarios but demand has begun to drive their adoption [36].

[36] Gartner. 2004. MCI's Denial of Service Response Offer May Start a Trend *www.gartner.com/resources/119900/119961/119961.pdf*

The following provisions should be expressly considered when entering into or reviewing agreements.

- IT outsourcers should be able to detect, analyse and mitigate DoS and DDoS attacks in a timely manner. While some DoS attacks are unable to be fully blocked without additional resource provisioning, the onus should be on the outsourcer to provide the expertise to analyse and apply mitigating controls if possible. It should also be agreed that DoS vulnerabilities in the configuration of systems and infrastructure should be removed as they become known. Furthermore, quality assurance programs can be used to alleviate existing DoS vulnerabilities.
- Internet/telecommunications service providers should provide a given level of availability, bandwidth and packet throughput. It is important that the bandwidth and packet-processing speeds are not a theoretical maximum but rather a constantly usable measure. Moreover, a guaranteed short response (not fix) time should be a priority, which may come at an additional cost to business.
- Hosting facilities should have the infrastructure to support the level of availability present in the SLA. Given that data centres are usually on the critical path of enterprise communications, support infrastructure such as uninterruptible power supplies, cooling, etc, must be in place. The Uptime Institute provides a clear classification of infrastructure requirements [37] for achieving varying levels of availability.
- Customers of critical infrastructure organisations often have service level requirements themselves. Before entering into any agreement, it is important to understand DoS-handling capability; that is, the technical, operational and strategic measures in place to cope with a DoS event.

Conduct Joint Exercises

The United States Department of Homeland Security (DHS) in 2006 carried out an exercise dubbed Cyber Storm, testing the country's preparedness for cyber attack [38]. As a result of the exercise, which involved 115 public and private sector organisations, some significant shortcomings were discovered in the ability of some entities to operate while under attack.

Members of Australian Government organisations have expressed interest in undertaking similar exercises locally or as part of the next Cyber Storm in 2008. Furthermore, exercises between inter-related critical infrastructure organisations, such as banks, clearing companies and the Reserve Bank, will be beneficial. Joint exercises can deliver real-world experience and an overall picture of critical infrastructure's ability to cope with a direct DoS attack.

Improve Information Sharing

Several of the critical infrastructure organisations interviewed for this project suggested that the availability and dissemination of DoS-related information between

[37] Turner IV, W, P. et al. 2005. Industry Standard Tier Classifications Define Site Infrastructure Performance. Uptime Institute. *www.upsite.com/file_downloads/PDF/Tier_Classification.pdf*
[38] Broache, A. 2006. Homeland Security wraps up first mock cyberattack. CNET *http://news.com.com/Homeland+Security+wraps+up+first+mock+cyberattack/2100-7349_3-6038082.html*

organisations is currently inadequate. Although the following initiatives provide excellent infrastructure for information to be shared, it is felt that specific DoS advice and data require greater focus.

- Trusted Information Sharing Network (TISN) including the IT Security Expert Advisory Group (ITSEAG)
- Information Security Incident Detection Reporting and Analysis Scheme (ISIDRAS)
- Australian Computer Emergency Response Team (AusCERT)

It is clear that many organisations are reluctant to share information regarding DoS incidents and experiences for fear of exacerbating the impact of previous attacks through introducing brand-related risks, and the likelihood of further attacks. However, it is recommended attempts be made to use the available information-sharing conduits to disseminate information to gain the following societal benefits:

- early warning of potential attacks;
- elimination of duplicate research;
- creation of a body of statistical data for risk/cost calculations; and
- availability of practical success strategies and technical measures (such as IDS/IPS signatures).

Obtain Insurance

Insurance can be an effective strategy in curbing the financial consequences of cyber insecurity. While still in its early development stages, cyber insurance provides a financial recourse for meeting the costs associated with cyber security incidents such as a DoS or DDoS attack. The adoption of these products has grown worldwide in the past five years, particularly in North America and Europe, but local adoption has been stalled by demand-side and supply-side impediments. [39]

For individual organisations, cyber insurance provides financial certainty to combat the variable-cost risk of cyber incidents. For example, the extent and the magnitude of potential loss through DDoS attacks is difficult to determine and would be highly volatile from year to year. Insurance provides the ability for organisations to transfer the cost and control this cost in the long term.

The benefits derived from cyber insurance—including the collection of actuarial data, greater monitoring and information sharing—will ultimately improve protective practices and curb the consequences of DoS and DDoS attacks through creating economic incentives.

Introduce Industry/Government Incentives

Internationally recognised security researcher Ross Anderson famously postulated that:

> "While individual computer users might be happy to spend $100 on anti-virus software to protect themselves against attack, they are unlikely to spend even

[39] Tan, B. 2006. Cyber Insurance and its Economic Viability. SIFT.

> $1 on software to prevent their machines being used to attack Amazon or Microsoft." [40]

Unless this economic disincentive is addressed, vast botnets are likely to continue to exist and grow.

Critical infrastructure bodies should adopt a strategy to discourage organisations and individuals from idly allowing their resources to be harnessed for attacks against others. This can be achieved through the application of legal, commercial, or social responsibility with a practical means of recourse against non-complying organisations and individuals.

One such initiative being trialled by the Australian Communications and Media Authority (ACMA) is the Zombie Hunting Program [41]. This is an internationally leading program to reduce the number of Australian computers controlled by attackers. Once a zombie is identified by ACMA, details are passed to the relevant ISP which is then responsible for contacting the customer and remedying the problem. If broadly adopted, such an initiative could significantly reduce the ability of attackers to conduct DDoS attacks in Australia since most zombies would have to be located overseas and traffic would necessarily traverse narrower international communications channels.

PROTECT

Protection from DoS attacks poses a difficult challenge. A single technology or operational process on its own will not provide adequate protection. Operational processes and technical mechanisms can be applied in tandem to harden an organisation against attack.

Operational

The following operational processes may be used to protect an organisation from DoS attacks:

- Including DoS in security testing scope
- Conducting technology risk assessments
- Completing bottleneck analysis
- Utilising secure application design
- Ensuring secure network design
- Capacity planning
- Ensuring physical security
- Removing reflectors and amplifiers
- Including DoS in business continuity management

[40] 2001. Anderson, R. Why Information Security is Hard – An Economic Perspective. *www.acsac.org/2001/papers/110.pdf*

[41] Fisher, V. 2006. Australians Go Zombie Hunting. *www.itnews.com.au/newsstory.aspx?CIaNID=20875*

Include DoS in Security Testing Scope

Regular testing cycles of all networked and high-value systems are likely to be already in place at most critical infrastructure organisations. Current processes should be updated or new process developed to specifically include DoS objectives.

As DoS issues can occur at many levels, testing must therefore occur at those levels to ensure no unnecessary risk is present. A thorough testing scheme should include the following, with some specific focus on Denial of Service vulnerabilities in each area:

- Network penetration testing to identify vulnerabilities in operating systems and software installations.
- Application penetration testing and code review to identify specific logic and programming errors that lead to DoS in custom and open source software.
- Physical security testing to verify that unauthorised personnel cannot physically disconnect or otherwise interrupt the operation of critical systems.
- Process and policy testing including social engineering to ensure that employees do not knowingly or unknowingly subvert control measures that are in place and that incident response processes are understood by staff and executed appropriately.
- Load and stress testing to identify the maximum throughputs that are achievable and sustainable and verify that various levels of attack will not greatly impact on system responsiveness.
- Telephony systems testing to certify that voice communications cannot be compromised.

Conduct Technology Risk Assessments

Any project that includes a technology-based component will require an analysis of technology risk. This includes all risks that may impact on the existing business, be introduced as a result of new systems, or affect the long-term technology strategy of the organisation. DoS is most often a technology risk.

A Technology Risk Assessment (TRA) will provide a means for prioritising DoS mitigation efforts. The most appropriate operational and technical controls can then be developed and applied.

Complete Bottleneck Analysis

DoS attacks that rely on the maximisation of consumption of finite resources, especially bandwidth, are by nature extremely effective at finding the weakest points of defence. Such attacks succeed because at some point in the chain of infrastructure, a component or set of components cannot process any additional load. Similarly, they also succeed because choke points and single points of failure are present.

Bottleneck analysis is crucial to an overall DoS protection strategy because a single bottleneck can render an entire protection scheme ineffective – for example, if a network is connected to the Internet at a speed of 100Mbs but the perimeter firewalls can only safely process 30Mbs of traffic.

Organisations can use testing and analysis to identify and remove bottlenecks. As every new bottleneck is removed, another component will become the bottleneck. This

process should be repeated until the bottleneck in the infrastructure meets minimum DoS protection requirements set by management.

Figure 11: Example Bottleneck Analysis shows a number of bottlenecks at different points in an arbitrary infrastructure. As these are alleviated in numerical order by the addition of capacity, they are replaced by further bottlenecks—the application bottleneck is replaced by the IPS bottleneck, and that in turn is replaced by the border firewall bottleneck.

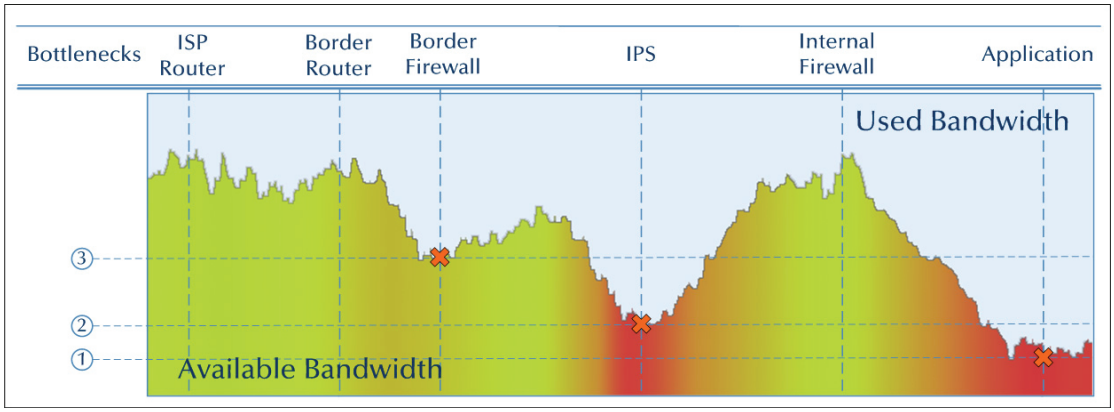

Figure 11: Example Bottleneck Analysis

Utilise Secure Application Design

Since applications have become some of the primary targets of DoS attacks, strong consideration must be given to the processes and techniques used to develop these applications. A number of best practices and principles are available to mitigate Denial of Service at the application level. Specifically, secure application design can counter attacks on business logic.

- **Simplicity**

  Excessive complexity of design and implementation is likely to introduce bugs into applications as expressed in the maxim "complexity is the enemy of security".

- **Defence in depth**

  The defence in depth paradigm [8] dictates that defences be applied at numerous points such that if one measure fails several more must still be defeated in order to fully compromise a system. This paradigm should be applied to application design to add controls at various levels of applications. In a common web application scenario these would include:

  - source code controls;
  - application server configuration;
  - protocols selection;
  - operating system configuration;
  - web server configuration; and
  - database design and configuration.

- **Coding standards**

  A coding standard is a document detailing the practices that must be observed by developers when writing code. By adhering to a best-practice standard, many

common vulnerabilities can be eliminated at the development stage and therefore reduce the risk of DoS issues.

- **Scalability**

  As load-based DoS attacks are often indistinguishable from genuine traffic, applications should be designed to scale with minimal effort and maximum gain. In the event that an organisation faces a sustained attack, further hardware can then be added to cope with the increased load.

- **Exception handling**

  One of the main causes of application DoS vulnerabilities is poorly designed exception handling. Best practice dictates that a 'catch-all' exception handler should be present and that errors should be handled as close as possible in the code base to where the exception occurs.

- **Logic that restricts access**

  Any application logic that restricts access to some users based on set criteria should be evaluated for DoS conditions. Often it is possible for an attacker to artificially create conditions meeting these criteria, hence denying access to legitimate users.

Ensure Secure Network Design

Analogous to secure application design, the following network design best-practice principles should be observed:

- Defence in depth
- Simplicity
- Scalability

Additionally, the following network design criteria will reduce DoS risk further:

- **Network and service segregation**

  If a DoS attack occurs, the scope and impact should be minimised. This can be achieved through the separation of networks and services at multiple levels. CERT/CC [33] recommends the following approaches:

  - Separating public services from private services
  - Splitting Internet, extranet, and intranet services
  - Dividing n-tier architectures into their components: web servers, application servers, database servers, and so on, with network control points (e.g. firewalls) separating each tier.
  - Using single-purpose devices for each service

  Further to this, it is important to understand the market positioning of key infrastructure providers to the organisation. For example, ensuring that the organisation's ISP provides segregation of business customers from home users can reduce exposure to many compromised 'local' systems. It is noted that programs such as the ACMA zombie hunt project are supporting ISPs in minimising the time a compromised system exists on an ISP's network.

- **Redundancy**

  Single points of failure create a high-risk exposure to DoS and therefore additional equivalent components should be available as an immediate replacement in the event of a component failure.

- **Load balancing**

  Load balancing mechanisms can be used to distribute the force of DoS attacks between several components and geographic locations so that no single component or network will receive the full volume of traffic.

- **Minimising attack space**

  CERT/CC suggests [33] "a well-implemented network can present a small target to attackers by limiting publicly visible systems and services to the minimum required to meet the business needs of the organisation". As such organisations should:

  - Block unnecessary incoming and outgoing traffic.
  - Deploy application proxies to limit malicious traffic.
  - Remove unused components and services.

- **Minimising external dependencies**

  Systems and networks external to an organisation cannot be directly controlled and therefore dependencies on them should be reduced as far as possible. Failure of the systems or networks depended on is likely to cause a DoS.

Plan for Capacity

A major Australian Internet infrastructure organisation has stated that capacity planning is imperative to defeating DoS. Critical infrastructure organisations should analyse network and application requirements in relation to current infrastructure to produce a baseline requirement for capacity. Once a baseline for 'normal' operation is created, additional capacity for handling DoS can be factored in. Discussions with ISPs and telecommunications service providers can ensure additional capacity is available as required.

At this level, it is not significant whether traffic surges are caused by malicious behaviour or legitimate external events. In fact, over-provisioning is the only truly effective means of defeating capacity-based attacks. However, it is typically not cost-effective and should be considered in line with available alternatives and cost-benefit modelling.

Additionally, CERT/CC cautions that [see 33] "most network devices and computer systems are limited not by raw bandwidth capacity (bits per second) but rather by their packet-processing ability (packets per second)."

Ensure Physical Security

Given that DoS can be perpetrated at the physical level, appropriate physical security measures are necessary. These should be implement inline with ISO 17799 Section 7 [see 35].

Remove Reflectors and Amplifiers

Individual organisations, particularly those with access to large bandwidth, such as telecommunications carriers, have a social responsibility to identify and remove (as far as possible) reflectors and amplifiers from their networks. The fewer of these that exist, the fewer avenues of anonymity and large-scale assault will be available to attackers.

Consequently the risk of DoS will be lowered for all critical infrastructure organisations.

The SANS Roadmap [see 34] recommends that "unless an organisation is aware of a legitimate need to support broadcast or multicast traffic it should be disabled". Furthermore, misconfigurations that cause other avoidable amplification or reflection of messages, such as recursive DNS queries, should also be remedied.

Include DoS in Business Continuity Management

Business Continuity Management (BCM) is the overarching process that manages the availability of critical business-enabling functions, operational and technical. BCM is a proactive strategy for managing the risk and consequences of an attack such as DoS. It requires the understanding of the business, along with the development, exercise and maintenance of Disaster Recovery and Business Continuity Plans (DR/BCP), as well as developing awareness throughout the organisation.

BCM elements, such as developing an Information Asset Register and conducting Business Impact Assessment (BIA) of risks, allow organisations to understand the threat of DoS attacks to their organisation. Through the development of BCPs which include contingency plans for various scenarios, BCM provides a mechanism for organisations to respond to and manage the consequences of DoS attacks as well as provide alternative processing. However, exercising these plans must be a key component of the BCM program. Whether the prescribed exercise is a desktop walkthrough or a full-scale DoS scenario drill, exercising of plans provides employees with experience in preparation for a disaster, as well as providing validation of BCM assumptions.

TECHNICAL

The following technical measures can be used to provide a degree of protection from DoS attacks to network and system resources:

- deploying anti-DoS devices and services;
- using egress filtering;
- applying ingress filtering;
- utilising timely patch management;
- deploying anti-virus software; and
- performing system hardening.

Deploy Anti-DoS Devices and Services

There are a number of devices and services which are part of a maturing market place for anti-DoS solutions. While imperfect, some of the solutions available have shown great resilience to even the largest, highly sustained attacks.

- Most devices offer both signature-based and statistical-based detection mechanisms which are best used in combination to deliver the lowest rate of false-positives and false-negatives. Prevention devices are usually placed at the extremities of the network while detection devices are closer to key infrastructure. There are a number of anti-DOS devices from service providers.

Managed DoS services are perhaps of greatest benefit to organisations with critical Internet-facing infrastructure because the onus to deliver high availability is on the

outsourcers. However, these services are not themselves immune and are usually offered at a high premium. Anti-DoS services are offered by:

Case Study : Akamai

What happened?

Hosting provider Akamai suffered a massive DoS attack on 15 June 2004. Microsoft, Apple, and Yahoo were among the large Akamai customers who suffered outages as a result of sharing infrastructure. The flood of traffic was directed against domain name service (DNS) systems causing name to IP address resolution to be slow for approximately two hours.

What was the impact?

While Akamai claims to work on a decentralised model with plenty of bandwidth to support even the largest attacks, it was not immune. About one per cent of its customers reported a significant impact affecting more than 20 per cent of their users.

How was the situation handled?

Tom Leighton, chief scientist at Akamai, said the attack was "so large that it [couldn't have] come from a couple of servers", and that "working with [their] network partners, [they] were able to identify a bot network that appeared to be operating and managed to shut it down, which resulted in stopping the attack". Having the resources and relationships in place helped to diffuse the situation promptly and restore full services to all customers.

Further information:

http://news.com.com/Blackout+hits+major+Web+sites/2100-1038_3-5234500.html

www.vnunet.com/vnunet/news/2125241/akamai-investigates-denial-service-attack

http://news.zdnet.com/2100-1009_22-5236403.html

www.theregister.co.uk/2004/06/15/akamai_goes_postal/

http://networks.silicon.com/webwatch/0,39024667,39121399,00.htm

Case Study 5: Akamai

Use Egress Filtering

Given that spoofing is a major contributor to Denial of Service, SANS [see 34] recommends:

> "User organisations and Internet service providers … ensure that traffic exiting an organisation's site, or entering an ISP's network from a site, carries a source address consistent with the set of addresses for that site."

Such an approach—if widely implemented—would have global benefits in reducing the number of hosts that could be used to launch anonymous attacks. The relevant filters are best applied at routers and firewalls at all levels of the network perimeter.

Apply Ingress Filtering

Ingress filtering can be used to ensure that many types of spoofed messages cannot enter a network. Like egress filtering, this should be applied at multiple levels using router ACLs and firewall rules. However, in this case many spoofed messages will not be identifiable as they will contain valid source addresses. Local addresses, internal

addresses and unallocated addresses are the major groups that should be disallowed access.

While ingress filtering can be used as a protective measure, it should also be used as a reactive measure if the source of attack can be clearly identified. In such a case, it is possible to disallow all messages from that source address from entering the network (although it must be noted that such an approach may interrupt a small amount of valid traffic).

Utilise Timely Patch Management

Timely patching of security vulnerabilities continues to be a problem. As a large number of bots are initially compromised through unpatched vulnerabilities, this is a significant root issue. It is recommended a patching process such as that provided by the United States National Institute for Standards and Technology [42] (NIST) be adopted to reduce the number of hosts vulnerable to compromise by DoS bots.

Deploy Anti-Virus

According to the Australian Computer Crime and Security Survey, 2005 [see 21], 99 per cent of organisations now employ anti-virus software as a protective technology. Deployment of anti-virus on all machines including individual desktops should be a part of organisational policy to prevent any machines being used as zombies.

Perform System Hardening

System 'hardening' is ideal for protecting computers from becoming infected with DoS attack tools and preventing application and operating system-specific Denial of Service vulnerabilities. The hardening process refers to applying best-practice configurations to systems to strengthen their security.

A number of thoroughly tested best-practice standards are available for various systems:

- Centre for Internet Security (CIS) Benchmarks [43]
- NSA Security Recommendations Guides [44]
- NIST Special Publications [45]
- Microsoft Security Guides [46]

DETECT

Given the range of attacks covered by DoS/DDoS, it is often difficult to know when an organisation is under attack. In the DoS case, the effects are likely to be immediate and result in some system or subsystem becoming unavailable. The symptoms of DDoS

[42] Mell, P. 2005. Creating a Patch and Vulnerability Management Program. NIST. *http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf*
[43] Center for Internet Security. 2006. CIS Benchmarks / Scoring Tools. *www.cisecurity.org/*
[44] National Security Agency. 2006. Security Configuration Guides. *www.nsa.gov/snac/index.cfm?MenuID=scg10.3.1*
[45] National Institute of Standards and Technology. 2006. Special Publications. http://csrc.nist.gov/publications/nistpubs/index.html
[46] Microsoft. 2006. Server Security. *www.microsoft.com/technet/security/topics/serversecurity.mspx*

attack may require a longer time to become visible and are usually apparent in the form of slow access times or service unavailability. DoS detection techniques are generally technical as opposed to process-based.

OPERATIONAL

Develop Anti-Virus Vendor Relationships

Anti-virus (AV) firms are leaders in malware research and possess detailed information about botnet sophistication and proliferation. AV vendors regularly infiltrate (due to their centralised control structure) some of the largest botnets in the world, gaining both active and passive access. They are therefore in the best position to predict, trace, and even shut down immediate threats to Australian critical infrastructure. For this reason, it is recommended strong relationships be established with AV vendors to keep abreast of the latest techniques and impending threats.

TECHNICAL

Technical mechanisms do not always accurately detect and identify DoS/DDoS attacks; however, when used in combination, a correlation of information can prove very effective. The following technical approaches can aid in attack detection:

- Deploying intrusion-detection systems
- Developing and deploying monitoring and logging mechanisms
- Deploying 'honeypot' systems

Deploy Intrusion Detection Systems

Intrusion Detection Systems (IDSs) have matured and are now extremely sophisticated and effective at detecting DoS attacks. Given that 59 per cent [see 21] of Australian organisations have existing IDS deployments, it is recommended that this be leveraged to place focus on DoS detection where appropriate.

Develop Monitoring & Logging

A critical infrastructure Internet solutions provider has highlighted a general lack of instrumentation for the forensic study of DoS attacks after their execution. It is recommended that organisations invest in technology which allows them to monitor relevant statistics in real time. Such data should also be logged to a centralised store for future correlation and analysis.

The following monitoring points are likely to aid in the analysis of DoS attacks:

- firewall packet logs and statistics;
- router statistics;
- systems performance counters such as CPU utilisation;
- ISP backbone performance data; and
- application logs.

However, there is a risk that the monitoring and logging functionality will in itself introduce dangerous bottlenecks and such systems must themselves be reviewed to ensure they cannot introduce DoS conditions to a system or device. For example, a

firewall logging all denied packets could fill log storage completely, creating a DoS condition depending on the fail-open or fail-closed configuration.

Deploy Honeypots

The success of the Honeynet project [see 27] in identifying botnets and tracking DDoS attacks demonstrates the value of honeypots as a DoS research tool. Organisations or service providers with a research capability should consider deploying honeypots as a means of understanding and protecting from cutting-edge DoS technology.

Any honeypots that are recruited into large botnets also offer greater social benefits as details can be reported to law enforcement and the botnets shut down. Furthermore, other organisations can be warned of impeding attacks on their infrastructure. There are, however, legal issues in deliberately deploying insecure technology for the purpose of trapping criminals. These should be investigated as appropriate by individual organisations.

REACT

Reaction to attack is likely to be of the greatest importance to many organisations but may be hampered by outsourcing and technical hurdles. Organisations must be well prepared to act in the event of a successful DoS attack.

Operational

'Reactive' operational processes generally revolve around incident response and analysis. As such, items recommended for consideration to improve operational response capability are:

- implement incident response planning;
- establish provider relationships; and
- perform attack analysis.

Implement Incident Response Planning

An incident response plan is vital to successfully handling a DoS attack. Such a plan defines people's roles and responsibilities in an incident situation, along with the processes that must be followed. The following actions should be taken when developing such a plan:

- Operating procedures—Document standard procedures that describe how people in each role should proceed during and after an incident to reduce the impact of the current attack, recover and protect against future attacks. Support tools and techniques should also be explained.
- Roles and responsibilities—Define the various roles of people during an incident, such as attack discoverer, media representative, network and systems administrators, business stakeholders, and law enforcement engagement manager. Assign hands-on responsibilities to each role and ensure limitations of authority are in place for each. Such a plan should also detail who can act in an emergency without explicit authorisation from superiors.
- Communication plans—Provide a detailed outline of what reporting processes must be followed. The sensitive nature of the information being communicated requires

a definition of what types of information should be provided to whom. This information should be classified according to its sensitivity, and handled accordingly.

Organisations interviewed have expressed the view that reporting structures are absolutely necessary for the specific case of DoS events. Typically, law enforcement should be contacted but organisations are often reluctant to do so. The Australian High Tech Crime Centre (AHTCC) is likely to be the most appropriate contact point. However, it has also been noted that in some cases AusCERT can expedite resolution of incidents arising overseas, through informal engagement with the relevant CERT at the source location.

Critical infrastructure organisations should also define a policy for contact with the media.

Case Study : FBI Investigations

What happened?

Beginning on October 6 2003 a number of young males were hired by Jay Echouafni, CEO of Orbit Communications, to launch DDoS attacks against various competitors. The attacks appear to have been motivated by the desire to increase market share but claims have also been made that revenge for similar attacks may have been a factor.

The attackers utilised SYN floods and HTTP floods from up to 15 000 zombies to overwhelm website communication links and even bring down parts of their ISP's infrastructure.

What was the impact?

One of Orbital's competitors, Weaknees.com, was effectively out of business for two consecutive weeks and suffered losses of $200 000. At the same time a second retailer, Rapid Satellite, was similarly attacked and affected.

However, the major impact was on an ISP who hosted one of the competitors. The ISP was inadequately equipped to handle the sheer volume of traffic generated by the attacks and for brief periods denied access to its major customers, Amazon.com and the Department of Homeland Security.

How was the situation handled?

The victims of these attacks several times migrated to ISPs with better infrastructure in an attempt to outlast the attacks, mostly without success. Finally, law enforcement was involved and in the first successful investigation of DDoS attacks in the United States charges have been brought against the responsible parties.

Further information:

www.securityfocus.com/news/9411

www.wired.com/news/privacy/1,68800-0.html

http://losangeles.fbi.gov/pressrel/2004/websnare082604.htm

Case Study 6: FBI Investigations

Establish Provider Relationships

Telecommunications service providers are often in the best position to provide practical protection, detection, filtering and tracing in the event of a DoS attack. It is therefore

important to establish and maintain a good working relationship with these providers. The quicker their reaction, the quicker the impacts of DoS can be mitigated.

Upstream providers will have greater resources than the customers to whom they provide services and can therefore shield customers from attack by implementing controls before malicious traffic reaches the customer. They are also able to provide performance data which may be vital to implementing additional measures at the organisation being attacked.

A good relationship with an upstream provider will also ensure that any sustained attack will not result in service to the organisation being discontinued. This is important because in an extreme case, it could be more cost effective for the provider to simply void a contract with a single client rather than continue adversely affecting its other customers.

Perform Attack Analysis

Analysing a DoS attack can be a difficult task but is necessary to react to a current attack and to prevent future attacks. To react to current attacks, analysis should concentrate on distinguishing malicious messages from legitimate ones. Once the criteria for such distinctions have been identified, the appropriate rules and filters can be applied as far upstream as possible.

CERT/CC recommends the following should be included as part of a post-mortem analysis:

- determining the attack type, source, and likely cause;
- determining the attack's effect on the intended target as well as collateral damage to other resources;
- gauging organisational reaction. Were appropriate people and resources allocated to the problem?;
- determining if documented processes were followed. Were they effective?;
- identifying how the attack was detected. Can detection be improved?;
- assessing the damages and determining the cost of the attack;
- determining legal recourse, if any; and
- assessing the responsiveness of external parties during the event.

TECHNICAL

A number of technologies can be deployed by organisations to respond to DoS or DDoS attacks. These include:

- deploying intrusion prevention systems
- applying rate limiting
- black-holing malicious traffic;
- using upstream filtering;
- increasing capacity; and
- redirecting domain names.

Deploy Intrusion Prevention Systems

Intrusion Prevention Systems (IPS) are Intrusion Detection Systems with the added functionality of being able to stop intrusion attempts when they are detected. IPS are very strong at detecting exploits of published DoS service vulnerabilities but they are unable to detect exploitation of business logic. As discussed in 'Attack Mechanics', evaluation of DoS attacks against business logic is integral to a holistic view of DoS threats. Furthermore, as the function of an IPS is to prevent many more forms of attack than just DoS, a DDoS flooding attack may overwhelm such a system if it is placed at the network edge or cause excessive false-positives if it is based on anomaly detection.

Apply Rate Limiting

If a network is the target of a flooding attack, all data flows which are identified as malicious or suspicious can be slowed to ease the strain on internal resources. Due to a common inability to isolate malicious DoS traffic, rate limiting is often the best approach to mitigating an attack because legitimate messages are not mistakenly discarded.

The limitation of this approach is that it protects only internal resources and not the edge of the network and associated bandwidth. Rate limiting can place a strain on the edge components which are performing the function and can cause delays to legitimate traffic.

Utilise Black-holing

Black-holing, or null routing, is the act of ignoring network communications based on set criteria. If analysis of a particular attack shows that DoS packets can be distinguished from legitimate packets by a particular characteristic, this characteristic can be used at the edge of the network or upstream provider to drop all malicious traffic without any response being provided to the source. As with rate limiting, this method does not protect any components or bandwidth upstream from its placement.

Use Upstream Filtering

Placing router and firewall filters as far upstream as possible can relieve pressure on subsequent infrastructure and is the most common method used to mitigate active DoS attacks. To implement effective upstream filters, a good working relationship is needed with upstream providers because not only is the implementation performed at the ISP level but the ISP may need to be engaged to perform analysis and tracing of the attack source in order to acquire the necessary details to complete this activity.

When engaging an ISP to perform analysis and filtering of a DoS attack, it is important to provide as much data and information as possible. This includes all relevant raw log data as well as the results of any analysis that has already been completed.

Increase Capacity

When other avenues of response have been exhausted, increasing capacity may be the only method of maintaining availability of systems in the face of a resource consumption attack. Capacity expansion should be considered for the following fundamental resources:

- bandwidth;

- processing (CPU) power; and
- storage capacity.

It should be noted that this can be the most expensive approach. Because it is likely that the capacity increase required is temporary, it is important to discuss with the organisation's telecommunications or Internet service provider, the availability of such capacity, the related costs and constraints regarding the availability of capacity, and engagement processes.

If an increase in capacity is implemented as a response to attack, a review of the capacity plan is recommended.

Redirect Domain Names

In some cases, attack tools are instructed to target a domain name rather than an IP address. If a targeted domain name is one of many and is not the primary name used to access a service, a short-term mitigation approach to alleviating attack impacts can be to modify or remove the IP address to which the domain name resolves.

CONCLUSION

The potential risk to a critical infrastructure organisation of being subjected to a DoS attack is too great to ignore. The losses in productivity, money and reputation can be significant. A well documented plan to deal with the threat is a necessity.

To counter this threat it is recommended organisations take the following actions:

- CEOs and Boards of Directors should understand the effect that a DoS, directed at either their organisation or at one of their trading partners, will have on their business;
- CIOs and security managers should ensure that the resources and procedures are in place to resist possible DoS attacks and plan for the continuity of the business through an attack; and
- Operational staff should seek further understanding of issues surrounding DoS and how they affect their organisations.

The key to successfully defending against DoS attacks is planning and preparation. A successful DoS risk management strategy will be in line with the defence in depth paradigm, which seeks to protect assets, detect attacks, and respond appropriately.

APPENDICES

APPENDIX A: GLOSSARY

- *Access Control List (ACL)*

  A mechanism for limiting access to a system resource to identities that have had such access authorised.
- *ACSI 33*

  The Australian Government Information and Communications Technology Security Manual, developed by the Defence Signals Directorate (DSD) to provide policies and guidance to Australian Government agencies on how to protect their ICT systems.
- *amplification*

  The process of increasing the volume of malicious traffic directed at the DoS target by using third-party resources.
- *back door*

  A hardware or software mechanism that provides an attacker access to a system and its resources without the need to further compromise the system.
- *bandwidth*

  The capacity of a communication channel to pass data through the channel in a given amount of time. Usually expressed in bits per second.
- *Black-holing*

  Discarding communication packets in a network, based on defined criteria.
- *bot*

  Short for 'robot'. An automated software program that can execute commands when provided by an attacker. In the context of a DoS attack, 'bot' generally refers to a software application running on a compromised machine which allows it to be used as part of an attack.
- *botnet*

  Short for 'robot network'. A network of bots, typically under the control of one attacker. Botnets can be used to launch a Distributed Denial-of-Service attack by an attacker commanding all the bots.
- *Business Continuity Management (BCM)*

  A holistic management process that identifies potential threats to an organisation and provides a framework for building resilience and the capability for an effective response.
- *Business Continuity Planning (BCP)*

  A subset of BCM, BCP is a methodology used to create a plan for ensuring continuous ability to carry out critical business processes, even under duress.
- *Domain Name System (DNS)*

  A network service that translates human readable domain names to their computer readable (IP address) equivalents.

- *false-positives/false-negatives*

  A false-positive is a test that mistakenly gives a positive reading; a false-negative mistakenly gives a negative reading. For example, a legitimate email that is mistakenly blocked by a spam filter is a false-positive, whereas a spam email that managed to evade the spam filter and be delivered is a false-negative.
- *flooding*

  An attack that attempts to cause a failure in a computer system or other data-processing entity by providing more input than the entity can process.
- *hardening*

  The process of strengthening the security of a system and its configuration.
- *honeypot*

  A deliberately vulnerable system (e.g. a web server) that is designed to be attractive to potential intruders.
- *Internet service provider (ISP)*

  An organisation that provides Internet access to other organisations or individuals.
- *Intrusion Detection System (IDS)*

  A system which detects anomalies in system and network behaviour for the purpose of identifying attacks.
- *Intrusion Prevention System (IPS)*

  A hardware or software system which detects and stops unauthorised activities.
- *ISO 17799*

  The International Standards Organisation *Code of Practice for Information Security Management.*
- Open Systems Interconnection Reference (OSI) Model

  An International Standards Organisation model for the development of interconnected systems.
- *Peer to Peer (P2P)*

  A decentralised networking paradigm under which all nodes function as both client and server to distribute information flows between nodes.
- *reflection*

  A method of disguising the source of an attack by ‘reflecting’ it off other servers on the Internet.
- *Service Level Agreement (SLA)*

  A formal agreement between a service provider and a customer to maintain a minimum level of service.
- *Supervisory Control and Data Acquisition (SCADA)*

  Systems used for remote monitoring and control in the delivery of utility services such as gas and water.
- *Top Level Domain (TLD)*

  Each domain name is made up of a series of character strings (called "labels") separated by dots. The right-most label in a domain name is referred to as its "top-level domain" (TLD).

- *social engineering*

  A euphemism for non-technical or low-technology means – such as lies, impersonation, tricks, bribes, blackmail, and threats – used to attack information systems, generally by manipulating the people involved in the system.

- *zombie*

  A computer infected with a bot and thus under the control of a remote attacker. Also see botnet.

- *Dynamic Host Configuration Protocol (DHCP)*

  A network protocol used to assign IP addresses to computers in a network and automatically configure related network settings.

APPENDIX B: KNOWN ATTACKS

Single-Point Denial of Service

Primary Category	Execution Approach	Definition	Typical Scenario
Physical Destruction or Alteration of Network Components	Power cut-off	Any event that causes loss of electrical or other source of power	An unauthorised person enters a data centre and unplugs power to critical server systems
Physical Destruction or Alteration of Network Components	Server shut-down	Unauthorised shutdown of a server machine	An unauthorised person enters a data centre and manually initiates the shutdown sequence on a machine
Destruction or Alteration of Configuration Information	Domain name theft	Transfer of a domain name to an illegitimate owner	An unauthorised person calls a domain registrar and transfers domain rights to themselves. Subsequently the domain is rerouted to a phishing scam
Destruction or Alteration of Configuration Information	Remote registry editing	Modification of the Microsoft Windows registry to stop Windows from functioning correctly	If remote registry access is enabled, an attacker may be able to modify configuration settings over the network
Destruction or Alteration of Configuration Information	DNS cache poisoning	Modification of the Domain Name Service cache causing domain name redirection	Several vulnerable DNS servers are poisoned and domain names resolve to phishing sites
Destruction or Alteration of Configuration Information	Local ARP poisoning	Changing the Address Resolution Protocol cache to reroute local network traffic	An attacker who has compromised a system on the DMZ poisons the ARP caches of other systems and impersonates the local gateway
Destruction or Alteration of Configuration Information	Local DHCP poisoning	Forcefully registering IP addresses to hosts that do not exist such that no more DHCP hosts can be assigned	Having compromised a system on the DMZ, an attacker uses this to start a lease on all IPs when a machine is rebooted, thus stopping it from regaining its lease
Attacks on Business Logic	User enumeration in combination with account lockout	Providing incorrect login information to list of known accounts several times to cause account lockout	An inexperienced attacker tries to get the password of any type of account, thus locking out many before being successful

Primary Category	Execution Approach	Definition	Typical Scenario
Attacks on Business Logic	Poor error handling	Supplying unexpected data to a system to cause it to crash or otherwise behave poorly	Garbage data is sent to a web service to stop it from responding, subsequently causing commercial partners to complain
Attacks on Business Logic	Mail bomb	Overwhelming the mail server with excessive numbers of emails.	A spam email organisation sends more email than a mail server can handle
Attacks on Business Logic	Client-side Denial of Service	Causing client software or systems to malfunction so that users are unable to connect to the server	An attacker initiating a network flood against a victim in order to take them off the network and subsequently impersonate them
Attacks on Business Logic	Wireless de-authentication	Spoofing a de-authentication message to cause a client to believe they have been disconnected from the wireless network	An attacker stands outside a building with a powerful antenna and broadcasts de-authentication packets, interrupting much of the wireless traffic
Using Your Own Resources Against You	UDP Packet Storm Attack	Spoofing UDP packets to services which always answer causing two to continually answer each other	An attacker sends thousands of packets to internet networks that accept broadcast addresses causing them to overload the targeted network
Using Your Own Resources Against You	Smurf Attacks	Spoofing packets to a broadcast address causing a great number of replies to be sent to the target	An attacker utilises a broadcast network to amplify an ICMP flood
Consumption of Other Resources	Application data structure consumption	Using faults in data structure implementation to make processing prohibitively slow	Supplying specially crafted data to an application in order to exploit weaknesses in internal table or tree data structures
Consumption of Other Resources	File system space Consumption	Causing a system to write large amounts of information to disk until storage capacity is reached	Causing an excessive number of error conditions to fill log files and therefore the disk on which they reside

Primary Category	Execution Approach	Definition	Typical Scenario
Consumption of Other Resources	Recursive XML entity attacks	Supplying recursive XML entity elements causing the parser to exhaust memory	An attacker supplies an XML document with recursive entity elements in order to consume memory on the server and halt processing
Consumption of Other Resources	Fork bombs	Creating execution processes that create more execution processes, exponentially consuming resources	Uploading an executable containing a fork bomb to a system for execution
Consumption of Other Resources	Large XML payload attacks	Stalling an XML parser by providing excessively large XML documents	An attacker supplies an excessively large XML document to an application for processing
Consumption of Other Resources	Internal/External entity references	Using XML to reference a file system in a way which is unexpected, causing the system to malfunction	Supplying an XML document containing a reference to the /dev/random file causing the parser to attempt to include its contents within the document
Consumption of Other Resources	Buffer overflows	Providing an application more data than has been allocated	An attacker supplies oversized data as an application input, overrunning a data buffer and corrupting the execution flow of the application
Consumption of Other Resources	LAND attacks	Certain Microsoft Windows systems cannot handle packets which have the same source and destination IP and port	Forging packets with identical source and destination addresses and sending them to a Windows system
Consumption of Other Resources	Session ID exhaustion	Exhausting the supply of session IDs available for users of an application	Initiating a large number of application sessions such that no more sessions IDs are available for new sessions
Consumption of Other Resources	Wireless bandwidth monopolisation	Abusing the wireless protocol to consume all the available bandwidth	An attacker connects to a wireless network and consumes all available bandwidth by abusing 802.11 management frames
Consumption of Other Resources	SMS Flooding	Sending excessive numbers of SMS messages to a mobile phone	A flood of SMS messages is delivered to the victim, overwhelming their mobile phone

DISTRIBUTED DENIAL OF SERVICE

Primary Category	Execution Approach	Definition	Typical Scenario
Bandwidth Consumption	Recursive DNS attacks	Sending spoofed DNS queries causing the DNS system to recursively send replies	An attacker spoofs DNS requests from the victim to open recursive DNS servers which amplify responses
Bandwidth Consumption	ICMP Flood	Sending large volumes of ICMP traffic, overwhelming the target	Launching an ICMP Ping flood against a system to consume its network bandwidth
Bandwidth Consumption	Smurf Attacks	Spoofing packets to a broadcast address from a number of sources causing a great number of replies to be sent to the target	An attacker sends millions of packets to broadcast addresses, each of which reply with a multiplied number of packets to the target
Bandwidth Consumption	Phone flood	Exhausting the phone lines of the target to prevent legitimate calls getting through	Using multiple phone lines to dial a particular number to overload the target
Using Your Own Resources Against You	Smurf Attacks	Spoofing packets to an internal broadcast address causing a great number of replies to be sent to the target internal addresses which may also cause other responses	Spoofing ICMP Ping request packets to internal broadcast addresses to elicit a flood of Ping replies to target systems
Using Your Own Resources Against You	Self-propagating worm	Malware that is capable of discovering additional targets to infect and executing an attack in order to spread	If a large number of networked computers become infected, the scanning activity from the worm may flood the network with spurious traffic
Network Connectivity	SYN Flood	Starting but not completing large numbers of TCP connections to a target	An attacker sends a large number of TCP SYN packets to the target in order to initiate a connection but does not complete or close the connection
Network Connectivity	UDP Flood	Sending large volumes of UDP	An attacker floods a target with UDP

Primary Category	Execution Approach	Definition	Typical Scenario
		packets to a target	traffic, consuming network bandwidth
Abuse of Business Logic	Uncompleted application transactions	Initiating excessive amounts of application-level transactions	Performing the initial stages of application transactions but not cancelling or completing them so that the application maintains the state of all the incomplete transactions
Network Connectivity	Teardrop attacks	Sending large volumes of IP packets which are fragmented and overlapping causing reassembly to become slow	Sending large numbers of large packets that are fragmented to a target
Network Connectivity	Connection reset attacks	Supplying TCP Reset packets to previously established connections	Terminating legitimate connections with spoofed connection reset packets
Network Connectivity	Authentication rejection attacks	Spoofing authentication replies causing the false appearance of authentication failure	Impersonating the server in order to spoof authentication failure messages
Network Connectivity	ICMP unreachable attacks	Supplying ICMP unreachable	Spoofing ICMP unreachable packets to deceive victims into thinking a connection could not be established due to a network connectivity issue
Consumption of Other Resources	Large XML payload attacks	Stalling an XML parser by providing excessively large XML documents from multiple sources	Sending large XML documents to an application for processing from multiple sources
Consumption of Other Resources	Recursive XML entity attacks	Supplying large amounts of recursive entity elements from multiple sources causing the parser to stall	Sending XML documents containing recursive entity elements to an application for processing from multiple sources
Consumption of Other Resources	File system space consumption	Using multiple senders to cause a	Sending malformed or s to a system from multip

Primary Category	Execution Approach	Definition	Typical Scenario
		system to write large amounts of information to disk until storage capacity is reached	force logging mechanis amounts of data and exl space

APPENDIX C: DOS TOOLS

Name	Type	Description
Trinoo	UDP	Only initiates UDP attacks to random ports. Communication between master and slave is via unencrypted TCP and UDP. No IP spoofing. Uses UDP ports 27444 and 31335. http://staff.washington.edu/dittrich/talks/cert/trinoo.analysis.txt
TFN	UDP, ICMP Echo, TCP SYN, Smurf	Uses IP spoofing. Uses ICMP Echo reply packets to communicate between zombie and master. http://staff.washington.edu/dittrich/misc/tfn.analysis.txt
Stacheldracht	UDP, ICMP, TCP SYN, Smurf, TCP ACK, TCP NUL	Uses encryption for communications and has an auto-update feature (via rcp). Has ability to test (via ICMP Echo) if it can use spoofed IP addresses. http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt
TFN 2K (Tribal Flood Network)	UDP, ICMP Echo, TCP SYN, Smurf	Same as TFN - but the slave is silent so difficult to spot. No return info from slave. Zombie to master communication is encrypted.
FAPI	UDP, TCP SYN, TCP ACK, ICMP	Can spoof IP addresses
Freak88	ICMP	NT specific zombie. No spoofing capabilities. Sends ICMP 1500 octet packets marked as fragments.
Shaft	UDP, ICMP, TCP SYN	Uses UDP ports 18753 and 20433. Has optional IP spoofing capabilities
Mstream	TCP ACK	Master connects via telnet to zombie. Communication between zombie and controller is not encrypted. The target gets hit by ACK packets and sends TCP RST to non-existent IP addresses. Routers will return ICMP unreachable causing more bandwidth starvation.
Blitznet	TCP SYN	Can spoof IPs and do IP flooding
Targa	ANY	Works by sending malformed IP packets known to slow down or hang up many TCP/IP network stacks.
Spank	Multicast	Will only work on a multicast-enabled network. Similar to Mstream.
Stick	Any	Stick uses the straightforward technique of firing numerous attacks at random, from random source IP addresses to purposely trigger IDS events. Stick is a DoS tool against IDS systems.
Omega	TCP ACK, UDP, ICMP, IGMP	Can spoof IPs and has a chat option between attackers
NAPTHA	TCP	Naptha attacks weaknesses in the way some TCP stacks and applications handle large numbers of connections in states other than "SYN RECVD," including "ESTABLISHED" and "FIN WAIT-1."

Name	Type	Description
Trinity (also called MyServer and Plague)	UDP, TCP Fragment, TCP SYN, TCP RST, TCP RandomFlag,TCP ACK, Establish, NULL	Listens to TCP port 33270. When idle it connects to Undernet IRC server on port 6667.
HTTPSmurf	TCP HTTP	Using public IIS servers as unsuspecting zombies, it sends a string of data to multiple web servers and they reflect the data to the target.
Power worm	TCP HTTP	Utilising an IIS Unicode support, this worm uses IRC as a back channel to control an army of zombies.
SQL — Voyager Alpha	TCP HTTP	Uses an SQL Server with no password (default) and takes over the system connecting it to an IRC botnet to DDOS victims.
Agobot / Gaobot / Phatbot / Forbot / Codbot / Toxbot / SDBot / RBot / Urot / UrXBot	TCP, UDP	Affects Windows systems, controlled through IRC channel, allows users to execute commands on the infected system, may steal personal information, can launch DDoS attacks on targets set by the user
mIRC Bots	TCP, UDP	Hides mIRC client application on the infected system for command and control through IRC channels, can launch DDoS attacks on targets set by the user
nugache	TCP, UDP	Controlled through unknown P2P network, may steal personal information, can launch DDoS attacks on targets set by the user

APPENDIX D: SUMMARY OF MANAGEMENT PRACTICES

Strategic	• Participate in DoS information-sharing networks such as TISN, ITSEAG and AusCERT • Run DoS scenarios to identify weaknesses - individually and also with business partners • Incorporate DoS into risk-management program • Implement proven security management framework • Create industry/government incentives • Promote DoS awareness and understanding in key staff through training • Negotiate service-level agreements with suppliers for DoS protection and response levels • Consider cyber-insurance • Negotiate Service Level Agreements around the DoS protection and response

	Operational	**Technical**
Protect	• Include DoS security in testing scope (IT Security Manager) • Complete technology risk assessments (IT Security Manager) • Complete bottleneck analysis on finite network resources (Network Architect/System Administrator) • Include security in application design (Application Architect) • Include security in network design (Network Architect) • Plan for capacity to endure DDoS attacks (Network Architect) • Implement appropriate physical security measures (IT Security Manager/Operation Manager) • Remove of reflectors and amplifiers (System Administrator) • Include DoS in business continuity management (Operations Manager)	• Utilise anti-DoS devices and services (Network Architect) • Apply ingress and egress filtering at network gateways(Network Architect) • Ensure rigorous patch management (System Administrator) • Ensure anti-virus controls are updated and effective (IT Security Manager/System Administrator) • Perform system hardening (System Administrator)
Detect	• Form co-operative relationships with anti-virus (IT Security Manager)	• Deploy Intrusion Detection Systems (IT Security Manager/Incident Response Team) • Develop monitoring & logging mechanisms (IT Security Manager/System Administrator) • Deploy Honeypot systems
React	• Form co-operative relationships with service providers (Operations Manager) • Establish DoS incident response plan (IT Security Manager) • Perform attack analysis (IT Security Manager/Operations Manager)	• Deploy intrusion prevention systems (IT Security Manager/Incident Response Team) • Implement rate limiting (System Administrator) • Apply black holing to drop malicious packets (Network Administrator) • Increase network/system capacity (System Administrator) • Redirect redundant domain names (System Administrator)

REFERENCES

[1] APEC. 2005. APEC Strategy to Ensure Trusted, Secure and Sustainable Online Environment.

[2] Attorney-General's Department. 2006. Trusted Information Sharing Network Website. *www.tisn.gov.au*

[3] Trusted Information Sharing Network. 2006. Managing DoS Attacks: Advice for CEOs and Boards of Directors. <<< URL to be provided >>>

[4] Trusted Information Sharing Network. 2006. Managing DoS Attacks: Advice for CIOs. <<< URL to be provided >>>

[5] Shirley, R. GTE / BBN Technology. 2000. Internet Security Glossary. RFC2828.

[6] Attorney-General's Department. 2006. Trusted Information Sharing Network: About Critical Infrastructure. *www.tisn.gov.au*

[7] Mirkovic, J and Reiher R. 2004. A Taxonomy of DDoS attack and DDoS Defense Mechanisms. *http://lasr.cs.ucla.edu/DDoS/ucla_tech_report_020018.pdf*

[8] NSA. Defense in Depth. *www.nsa.gov/snac/support/defenseindepth.pdf*

[9] Malachi Kenney. 2006. Ping of Death. *www.insecure.org/sploits/ping-o-death.html*

[10] ISO/IEC. 2000. Basic Reference Model: The Basic. Open Systems Interconnection. *www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=20269&ICS1=35&ICS2=100&ICS3=1*

[11] Waldegger, T. 2006. Mozilla Firefox HTML Parsing Null Pointer Dereference Denial of Service Vulnerability. *www.securityfocus.com/bid/17499*

[12] Zalewski, M. 2005. Microsoft Internet Explorer JPEG Image Rendering CMP Fencepost Denial of Service Vulnerability. *www.securityfocus.com/bid/14284*

[13] Apelt, S. 2005. Veritas Backup Exec Remote Agent Null Pointer Dereference Denial of Service Vulnerability. *www.securityfocus.com/bid/14021*

[14] CERT/CC. 1999. Denial-of-Service attacks. *www.cert.org/tech_tips/denial_of_service.html*

[15] SecurityFocus. 2005. Microsoft Windows Plug and Play Denial of Service Vulnerability. *www.securityfocus.com/bid/15460/exploit*

[16] David Dittrich. 1999. The DoS Project's 'Trinoo' distributed Denial of Service attack tool. *http://staff.washington.edu/dittrich/misc/trinoo.analysis*

[17] infectionvectors.com. 2004. Agobot and the "Kit"chen Sink. *www.infectionvectors.com/vectors/Agobot_&_the_Kit-chen_Sink.pdf*

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

[19] Wikipedia. 2006. Slashdot Effect. *http://en.wikipedia.org/wiki/SlashDot_Effect*

[20] Peter Grabosky. 2000. Cyber crime and information warfare. *www.aic.gov.au/conferences/transnational/grabosky.pdf*

[21] AusCERT. 2005. Australian Computer Crime & Security Survey.

[22] Cobb, A. 1998. Thinking about the Unthinkable: Australian Vulnerabilities to High-Tech Risks. *www.aph.gov.au/library/pubs/rp/1997-98/98rp18.htm*

[23] Swiss Federal Institute of Technology. 2004. International CIIP Handbook 2004.

[24] Swiss Federal Institute of Technology. 2006. International CIIP Handbook 2006.

[25] ICANN Security and Stability Advisory Committee. 2006. DNS Distributed Denial of Service (DDoS) Attacks. SSAC Advisory SAC008. *www.icann.org/committees/security/dns-ddos-advisory-31mar06.pdf*

[26] The Honeynet Project & Research Alliance. 2005. Know Your Enemy: Tracking Botnets. *www.honeynet.org/papers/bots/*

[27] Sophos. 2005. Suspected zombie kings who ran botnet of 100,00 PCs arrested, reports Sophos. *www.sophos.com/pressoffice/news/articles/2005/10/va_dutchbotarrests.html*

[28] Papparlardo, D. and Messmer, E. 2005. Extortion via DDoS on the Rise. Network World. *www.networkworld.com/news/2005/051605-DDoS-extortion.html*

[29] ITSEAG. 2005. Security of Voice over Internet Protocol.

[30] ITSEAG. 2005. Wireless Security.

[31] Steve Martin. 2001. Anti-IDS Tools and Tactics. *www.sans.org/rr/whitepapers/detection/339.php*

[32] Attorney-Generals Department. 2005. SCADA Security – Advice for CEOs. Trusted Information Sharing Network.

[33] CERT/CC. 2001. Managing the Threat of Denial of Service Attacks. *www.cert.org/archive/pdf/Managing_DoS.pdf*

[34] SANS. 2000. Consensus Roadmap for Defeating Distributed Denial of Service Attacks. *www.sans.org/dosstep/roadmap.php*

[35] ISO. 2005. ISO 17799: Code of Practice for Information Security Management

[36] Gartner. 2004. MCI's Denial of Service Response Offer May Start a Trend. *www.gartner.com/resources/119900/119961/119961.pdf*

[37] Turner IV, W, P. et al. 2005. Industry Standard Tier Classifications Define Site Infrastructure Performance. Uptime Institute. *www.upsite.com/file_downloads/PDF/Tier_Classification.pdf*

[38] Broache, A. 2006. Homeland Security wraps up first mock cyberattack. CNET. *http://news.com.com/Homeland+Security+wraps+up+first+mock+cyberattack/2100-7349_3-6038082.html*

[39] Tan, B. 2006. Cyber Insurance and its Economic Viability. SIFT.

[40] 2001. Anderson, R. Why Information Security is Hard – An Economic Perspective. *www.acsac.org/2001/papers/110.pdf*

[41] Fisher, V. 2006. Australians Go Zombie Hunting. *www.itnews.com.au/newsstory.aspx?CIaNID=20875*

[42] Mell, P. 2005. Creating a Patch and Vulnerability Management Program. NIST. *http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf*

[43] Center for Internet Security. 2006. CIS Benchmarks / Scoring Tools.
www.cisecurity.org/

[44] National Security Agency. 2006. Security Configuration Guides.
www.nsa.gov/snac/index.cfm?MenuID=scg10.3.1

[45] National Institute of Standards and Technology. 2006. Special Publications.
http://csrc.nist.gov/publications/nistpubs/index.html

[46] Microsoft. 2006. Server Security.
www.microsoft.com/technet/security/topics/serversecurity.mspx