



Trusted Information  
Sharing Network  
for Critical Infrastructure Protection

---

**Denial of Service/Distributed Denial of Service**

## **MANAGING DOS ATTACKS**

### **ADVICE FOR CIOS**

June 2006

DISCLAIMER: To the extent permitted by law, this document is provided without any liability or warranty. Accordingly it is to be used only for the purposes specified and the reliability of any assessment or evaluation arising from it are matters for the independent judgment of users. This document is intended as a general guide only and users should seek professional advice as to their specific risks and needs.



## Executive Summary

The frequency and sophistication of Denial of Service (DoS) attacks, including a specific type known as Distributed DoS, are rapidly increasing. DoS attacks have left large corporate web sites inaccessible to customers, partners and users for hours or days, resulting in large financial losses. A comprehensive DoS management framework structured around the Protect, Detect and React triad is required to address the complete lifecycle of a DoS attack: strengthening systems and networks against attacks, detecting attacks when they occur and reacting appropriately to counter current and future attacks.

The information in this paper analyses the key areas of Threat assessment and Threat management, and provides best-practice recommendations for identifying DoS risks and the introduction of adequate protection measures.

This document has been developed by the IT Security Expert Advisory Group (ITSEAG), which is part of the Trusted Information Sharing Network (TISN)<sup>1</sup> for critical infrastructure protection and is one of three related reports:

- a paper for CEOs and Boards of Directors<sup>2</sup>;
- this CIO paper; and
- a detailed report<sup>3</sup> with a full analysis of the threats and countermeasures for DoS attacks.

---

<sup>1</sup> 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 oversees the IAAGs and EAGs). More on TISN can be sought from [www.tisn.gov.au](http://www.tisn.gov.au) or by contacting [cip@ag.gov.au](mailto:cip@ag.gov.au).

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

<sup>2</sup> Trust Information Sharing Network. 2006. Managing DoS Attacks: Advice for CEOs and Boards of Directors. [www.tisn.gov.au](http://www.tisn.gov.au)

<sup>3</sup> Trusted Information Sharing Network. 2006. Managing DoS Attacks: In-depth Report. [www.tisn.gov.au](http://www.tisn.gov.au)

## What is a Denial of Service attack?

Internet-dependent and networked infrastructure components are at risk of a Denial of Service (DOS) attack designed to render a system or network unusable. The ultimate aim of a DoS attack is to prevent users from accessing a system or resource, and the potential cost to critical infrastructure is considerable. The impact of downtime to critical infrastructure organisations may not be limited to lost revenue and goodwill, but can extend to social and human costs.

### *What can be done to protect the organisation?*

The threat of a DoS attack is most effectively addressed as a risk-management issue, and considered as an overall business risk, as opposed to a technical or operational risk. There are two key steps in an effective DoS threat mitigation strategy:

- Threat assessment
- Threat management

This document will guide an organisation through the process of assessment and management of DoS attacks by identifying the risk present and the appropriate measures that should be employed to protect valuable resources. The document should be read in conjunction with other recent work by the TISN. In particular the *Best practice, management and governance for IT and information security guidelines for corporate and business* guidance paper for CEOs and Boards of Directors<sup>4</sup>, and advice for CIOs<sup>5</sup>.

## Key questions to consider

These questions are designed to encourage discussion on the organisation's preparedness for a DoS attack. Answers to these questions should underpin the development of a comprehensive DoS risk-mitigation strategy.

### Questions to expect from your CEO

- How prepared are we and our trading partners to resist a DoS attack?
- What systems, connections and applications are most at risk?
- Do we have the resources to implement an effective DoS mitigation strategy?
- Have we provided our staff with the knowledge and tools to detect and respond to a DoS attack?
- Would our organisation benefit from participating in an industry-wide preparedness test?
- What are our contingency plans in the event that service has been denied to us?

---

<sup>4</sup> Trusted Information Sharing Network, 2006. Best practice, management and governance for IT and information security guidelines for corporate and business: Advice for CEOs and Boards of Directors. [www.tisn.gov.au](http://www.tisn.gov.au)

<sup>5</sup> Trusted Information Sharing Network, 2006. Best Practice, management and governance for IT and information security guidelines for corporate and business: Advice for CIOs. [www.tisn.gov.au](http://www.tisn.gov.au)

### Questions you should ask

- Which resources would be potential targets for attackers?
- Where are these resources vulnerable to attack?
- What frameworks are in place to protect vulnerable resources against a DoS attack?
- How can we recognise a DoS attack?
- How effective would our response be to a DoS attack?
- How much can we depend on our service providers to help in protecting, detecting and responding to DoS attacks?
- Can a denial of service against others affect us?
- Do our contracts with providers allow us to expand our resource usage if required?
- Do our current Business Continuity Plans cover a loss of Internet connection?

To answer the above questions, there are two key areas of review and action:

| Threat assessment   | Threat management   |
|---|---|
| <ul style="list-style-type: none"> <li>• Risk identification</li> <li>• Weaknesses exploited</li> <li>• Motivation of attackers</li> <li>• Attack trends</li> </ul> | <ul style="list-style-type: none"> <li>• Available resources</li> <li>• Strategic controls and responses</li> <li>• Strategy of protect, detect, react</li> </ul> |

The DoS management framework presented provides coverage of security before 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 attacks;
- Detecting attacks when they occur;
- Responding appropriately to counter current and future attacks; and
- Threat assessment.

The Threat Assessment identifies the DoS risks to critical infrastructure. Following the AS 4360 Standard for Risk Management is considered best practice. 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.

#### *Risk Identification*

At first glance, DoS attacks appear simple to define and distinguish; however, they can be categorised and sorted in numerous overlapping ways. The important distinctions are:

- **Attack vectors**—Services subject to DoS attacks are not restricted to the electronic medium; people can be ‘socially engineered’ and procedural loopholes can be abused.
- **Single point vs. distributed**—The aim of a DoS attack is to abuse specific vulnerabilities in business logic or system components. A Distributed DoS (DDoS)

typically involves using a number of previously compromised computers to attack the target. A DDoS attack can be more difficult to defend against and detect. Reaction to a DDoS attack usually requires the help of the organisation's external service providers.

- **Client vs. server**—Compromising a networked service or functionality can be achieved either by impeding the ability of the server to provide the service or by impeding the client's ability to access the service. DoS attacks against the server are by far the most common, with the intention of affecting all clients of a resource rather than a particular subset.
- **Communication layers**—It is possible to target any of the seven OSI communications layers because there is no electronic medium without an attack vector. Attacks directed at the higher layers are generally more sophisticated and harder to detect and prevent.
- **Attack mechanics**—For any DoS attack, it is important to ask “how was the attack executed?” and the most widely accepted categories are:
  - Consumption of scarce resources, such as network connectivity and bandwidth consumption;
  - Destruction or alteration of configuration information;
  - Physical destruction or alteration of network components; and
  - Abuse of business logic.
- **Tools**—DoS and DDoS tools are readily available, from simple single-target exploits to sophisticated self-propagating DDoS bots which are similar to Internet worms.
- **Weaknesses Exploited**—Most DoS attacks, especially distributed attacks, take advantage of fundamental weaknesses in computing infrastructure:
  - insecure systems;
  - lack of authentication;
  - existence of reflectors/amplifiers; and/or
  - problematic attack identification.

#### *Motivation for Attack*

DoS attacks began to occur when a critical mass of organisations and individuals became Internet connected, giving attackers real incentive to strike:

- credibility with other hackers for compromising a high-profile site;
- retaliation for real or perceived slights or injustices;
- monetary gain (criminal extortion or competitive tactics);
- the growing threat of political activism and cyber terrorism; and
- many DoS attacks are the result of simple boredom or ‘experimenting’ with new attack techniques.

### Attack Trends

The following summarises current and future trends in DoS attacks:

#### Current:

- Reflection and amplification
- Autonomous propagation
- Larger botnets
- Botnet markets
- Organised crime

#### Future:

- Attacks on emerging technologies
- Application layer
- Peer-to-peer botnets
- Realistic behaviour
- Attacks against anti-DoS infrastructure
- Attacks against SCADA systems

### 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 mis-configured 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.

#### Further information:

[www.icann.org/committees/security/dns-DDoS-advisory-31mar06.pdf](http://www.icann.org/committees/security/dns-DDoS-advisory-31mar06.pdf)

[www.news.com.com/New+denial-of-service+threat+emerges/2100-7349\\_3-6050688.html](http://www.news.com.com/New+denial-of-service+threat+emerges/2100-7349_3-6050688.html)

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

#### 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.

## Threat management

Developing an effective DoS threat-management strategy is a significant task. Therefore, focusing on key operational infrastructure rather than attempting to protect all systems from all DoS threats is the most productive approach.

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

- Outsourcing your business operations may rely on systems and networks over which you have no control.
- Interconnectedness it is not possible for one organisation to implement a unilateral strategy to provide full protection from DoS.
- Flood-based attacks some attacks can exactly mimic normal user behaviour and can only be treated by adding additional capacity.

### *Available Resources*

A considerable amount of work has been done in establishing strategies to cope with DoS and other malicious attacks. Following the frameworks for DoS management will not only help to protect against DoS attacks but the flow-on effects to organisational security will be noticeable. These frameworks include:

- CERT/CC, *Managing the Threat of DoS Attacks* (2001) 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 lifecycles.
- *Consensus Roadmap for Defeating DDoS Attacks* (2000), developed by the Project of the Partnership for Critical Infrastructure Security in the United States, describes the problems and suggests remediation measures.
- ISO 17799 *Code of Practice for Information Security Management* outlines best practices for organisational protection of information resources. Aligning practices with these requirements will aid in the overall management of DoS threats.
- ACSI 33 *Australian Government Information and Communication Technology Security Manual* provides policies and guidance to Australian Government agencies on how to protect their ICT systems.

### *Strategic Controls and Responses*

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
- Participating in joint exercises
- Improving information sharing
- Obtaining Insurance
- Encouraging industry / government collaboration

## PROTECT

Protection from DoS attacks poses a challenge because no single technology or operational process will provide adequate protection.

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

- conducting technology risk assessments;
- capacity planning;
- ensuring secure network design;
- ensuring physical security;
- utilising secure application design;
- including DoS in business continuity management; and
- including DoS in security testing scope.

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

- deploying anti-DoS devices and services;
- traffic filtering;
- utilising timely patch management;
- deploying anti-virus software; and
- performing system hardening.

## DETECT

Given the range of attacks covered by DoS/DDoS, 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.

One **operational** measure is to develop relationships with key sources of current IT security intelligence. Anti-virus firms are leaders in malware research and possess detailed information about botnet sophistication and proliferation. These firms along with groups such as AusCERT are in a good position to predict, trace and even work to shut down immediate threats to Australian critical infrastructure. For this reason, it is recommended strong relationships be established with key security resources to keep abreast of the latest techniques and impending threats.

The following **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; and
- deploying honey-pot systems to lure attackers away from the real systems.

## REACT

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

‘Reactive’ **operational** processes generally involve incident response and analysis. As such, items recommended for consideration to improve operational response capability are:

- Implementing incident response planning to define people’s roles and responsibilities, and the processes to be followed in an incident situation.
- Establishing relationships with telecommunications and internet service providers as these organisations can provide practical protection, detection, filtering and tracing in the event of a DoS attack.
- Performing attack analysis to react to a current attack and to prevent future attacks.

**Technical** measures which can be deployed by organisations to respond to DoS or DDoS attacks include:

- Using upstream filtering to relieve pressure on subsequent infrastructure. This is the most common method used to mitigate active DoS attacks.
- Deploying Intrusion Prevention Systems (IPS) to automatically stop intrusion attempts when they are detected.
- Applying rate limiting to ensure that legitimate messages are not mistakenly discarded.
- Black holing malicious traffic to ignore network communications based on criteria that were identified in the attack analysis.
- Increasing capacity to maintain availability of systems in response to a resource consumption attack.
- Redirecting domain names as a short term mitigation approach to alleviating attack impacts by modifying or removing the IP address the domain name resolves to.

## Conclusion

Denial of service attacks are a real threat to the operation of any networked computer system. While they can be difficult to detect and react to, prudent planning and preparation can mean the difference between a total shut down of the organisation and a slight inconvenience. Following the recommendations contained in this paper will provide the organisation with a solid base for minimising the impact of these potentially damaging attacks.

### Summary of recommended actions

|                  |  |
|------------------|--|
| <b>Strategic</b> | <ul style="list-style-type: none"> <li>• Incorporate DoS into risk-management program</li> <li>• Negotiate service-level agreements with suppliers for DoS protection and response levels</li> <li>• Consider running DoS scenarios to identify weaknesses (individually and also with business partners)</li> <li>• Participate in DoS information-sharing networks such as TISN, ITSEAG and AusCERT</li> </ul> |
|------------------|--|

|                | <b>Operational</b>   | <b>Technical</b>   |
|----------------|--|--|
| <b>Protect</b> | <ul style="list-style-type: none"> <li>• Include DoS security in testing scope (IT Security Manager)</li> <li>• Complete bottleneck analysis on finite network resources (Network Architect/System Administrator)</li> <li>• Include security in application and network design (Application/Network Architect)</li> <li>• Plan for capacity to endure DDoS attacks (Network Architect)</li> <li>• Implement appropriate physical security measures (IT Security Manager/Operation Manager)</li> <li>• Include DoS in business continuity management (Operations Manager)</li> </ul> | <ul style="list-style-type: none"> <li>• Utilise anti-DoS devices and services (Network Architect)</li> <li>• Apply ingress and egress filtering at network gateways (Network Architect)</li> <li>• Ensure rigorous patch management (System Administrator)</li> <li>• Ensure anti-virus controls are updated and effective (IT Security Manager/System Administrator)</li> <li>• Perform system hardening (System Administrator)</li> </ul> |
| <b>Detect</b>  | <ul style="list-style-type: none"> <li>• Create strong relationships with anti-virus vendors to keep abreast of the latest techniques and potential attacks (IT Security Manager)</li> </ul>   | <ul style="list-style-type: none"> <li>• Deploy intrusion detection systems (IT Security Manager/Incident Response Team)</li> <li>• Develop monitoring &amp; logging mechanisms (IT Security Manager/System Administrator)</li> </ul>  |
| <b>React</b>   | <ul style="list-style-type: none"> <li>• Form co-operative relationships with service providers (Operations Manager)</li> <li>• Establish DoS incident response plan (IT Security Manager)</li> <li>• Perform attack analysis (IT Security Manager/Operations Manager)</li> </ul>  | <ul style="list-style-type: none"> <li>• Deploy intrusion prevention systems (IT Security Manager/Incident Response Team)</li> <li>• Implement rate limiting (System Administrator)</li> <li>• Apply black holing to drop malicious packets (Network Administrator)</li> <li>• Increase network/system capacity (System Administrator)</li> <li>• Redirect redundant domain names (System Administrator )</li> </ul>                         |

Further information is available at the TISN website ([www.tisn.gov.au](http://www.tisn.gov.au)), including:

- Managing DoS Attacks: In-depth Report [PDF](#) | [WORD](#)
- National Strategy for Critical Infrastructure Protection [PDF](#) | [WORD](#)

Information for CEOs

- Managing DoS Attacks: Advice for CEOs and Boards of Directors [PDF](#) | [WORD](#)
- Best practice, management and governance for IT and information security guidelines for corporate and business—CEO Report [PDF](#) | [WORD](#)
- GPS—An Overview for CEOs [PDF](#) | [WORD](#)
- SCADA—Advice for CEOs [PDF](#)
- Security of Voice Over Internet Protocol—Advice for CEOs [PDF](#)
- Wireless Security—Overview for CEOs [PDF](#) | [WORD](#)

Information for CIOs

- Best practice, management and governance for IT and information security guidelines for corporate and business—CIO Report [PDF](#) | [WORD](#)
- Security of Voice Over Internet Protocol—Advice for CIOs [PDF](#)
- Wireless Security—Overview for CIOs [PDF](#) | [WORD](#)