Trusted Information Sharing Network
for Critical Infrastructure Protection

Managing Denial of Service (DoS) Attacks

Summary Report for CIOs and CSOs

December 2009

Executive Summary

As organisations continue to incorporate the Internet as a key component of their operations, the global cyber-threat level is increasing. As part of its *Cyber Security Strategy*, the Australian Government has recognised the need for Australian businesses to operate secure and resilient information and communications technology environments[1].

One of the most common types of cyber-threats to these environments is known as a Denial of Service (DoS) attack – an attack preventing users from accessing a system for a period of time. Recent DoS attacks have left large corporate and government web sites inaccessible to customers, partners and users for hours or days, resulting in significant financial, reputational, and other losses. The growing use of cloud computing services and shared infrastructure is further increasing the importance of having a considered plan for managing such DoS attacks.

Developing an effective mitigation strategy is an important measure to minimise the risk posed to an organisation by the threat of DoS attacks. 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.

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.
- Reacting appropriately to counter current and future attack trends.

Developing an effective DoS threat-management strategy is a significant task and one that requires extensive communications with partners and suppliers – particularly Internet and telecommunications service providers – prior to an incident occurring.

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.

Introduction

The ultimate aim of a DoS attack is to prevent users from accessing a system or resource, and the potential cost to critical infrastructure can be 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. Internet-dependent and networked infrastructure components are generally most at risk of a DoS attack.

---

[1] Australian Government, *Cyber Security Strategy*, 2009, http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(4CA02151F94FFB778ADAEC2E6EA8653D)~AG+Cyber+Security+Strategy+-+for+website.pdf/$file/AG+Cyber+Security+Strategy+-+for+website.pdf

A sufficiently motivated and skilled attacker may be able to commandeer adequate resources to overwhelm an organisation's infrastructure regardless of its level of preparedness. However, implementing an appropriate framework to manage the DoS threat can maximise the robustness of systems and minimise their downtime in the event of an attack.

There are three papers in this series:

- The full report which provides an introduction to the DoS threat to critical infrastructure and establishes a framework which details a governing strategy and recommendations at both operational and technical levels to protect, detect and respond to DoS attacks.
- The CEO paper, which provides an outline designed to provide senior executives and Directors of Critical Infrastructure organisations with guidance on the processes associated with managing DoS attacks.
- This CIO paper, which summarises the full report and contains a deeper analysis than the CEO paper of operational issues associated with managing DoS attacks

Threat Assessment

A Threat Assessment is the most effective way to identify the DoS risks to your organisation. Following the AS 4360 Standard for Risk Management is considered best practice. Firstly, the context of DoS as relevant to your organisation is established, then attack vectors are identified, followed by an analysis of risk, and finally the evaluation of those risks, as illustrated in Figure 1, below.

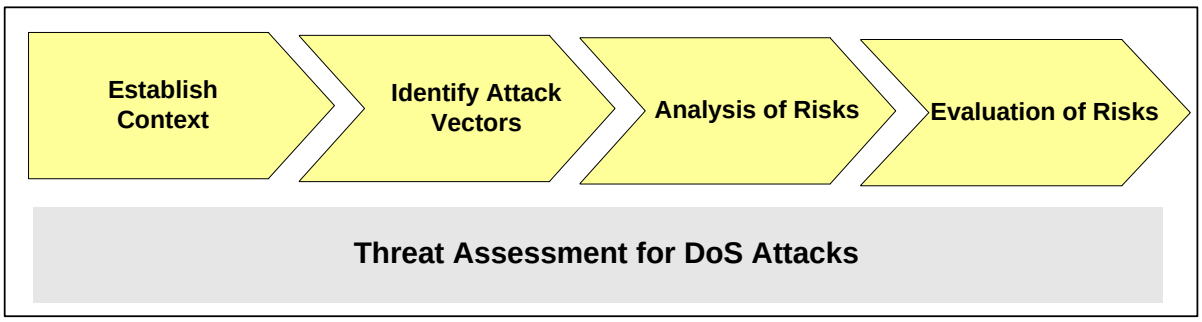

Figure 1 – High Level AS 4360 Risk Assessment Model

This section provides information to help organisations identify potential DoS targets in their business operations and IT environments, qualify the level of risk these targets are subject to, and consider the evolution of technology and threats and how this will change the risk assessment over time.

At first glance DoS attacks appear simple to define and distinguish; however, they can be categorised and sorted in numerous overlapping ways, and have a variety of very important factors to consider when assessing likelihood and impact. 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. In addition, pre-existing relationships between organisations can be exploited by attackers and leveraged in DoS attacks. For example, domain names can potentially be hijacked if an attacker is able to convince a domain name registrar to point a URL belonging to an

organisation to an IP address controlled by the attacker. This prevents the web site of that organisation from being accessible to legitimate Internet users.

- **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.
  - Abuse of business logic.
- **Single point vs. distributed** – The aim of a DoS attack is to abuse specific weaknesses in business logic or system components. A Distributed DoS (DDoS) typically involves using a number of previously compromised computers to attack a 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.
- **External vs. internal** – DoS incidents can originate both from sources external to an organisation, or from within the organisation itself. Internal incidents can include the deliberate acts of disgruntled employees, inadvertent acts such as mis-configuration of systems or through internal security incidents that affect the availability of systems.
- **Internally managed vs outsourced** – Your business operations may rely on systems and networks over which you have little or no control, especially with the increasingly common use of cloud computing services and Software as a Service (SAAS). In such an environment, protective measures implemented by external service providers are also important for an organisation to consider.
- **Communication layers** – It is possible to target any of the seven OSI communications layers. Attacks directed at the higher layers (particularly the application layer) are generally more prevalent, sophisticated and harder to detect and prevent.
- **Weaknesses Exploited** – Most DoS attacks, especially distributed attacks, rely on fundamental weaknesses in computing infrastructure:
  - Unpatched systems
  - Lack of authentication
  - Poorly configured systems (including virtual systems)
  - Existence of reflectors/amplifiers
  - Difficulties in identifying an attack
  - Shared, vulnerable infrastructure
- **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. Their motivations include:
  - 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)
  - Political activism and cyber terrorism
  - Simple boredom, a desire for entertainment, or 'experimenting' with new attack techniques

Some organisations may also be unintended targets for a DoS attack, either through a misdirected attack or sharing infrastructure with the intended target. Even in these cases, an appropriate strategy will still need to be in place to respond to such an attack.

- **Scope of attack** – While a DoS attack may be targeted against a specific component of an organisation's infrastructure (for example, its public website), the attack may also affect other systems as well (for example, the ability to send and receive email).

Attack Trends

The following summarises current and future trends in DoS attacks for use in identifying current DoS threats, and how these are likely to evolve over time:

Current:

- Reflection and amplification (including DNS recursion)
- Larger botnets & autonomous propagation
- Botnet markets which are increasingly sophisticated in nature
- Peer-to-peer botnets
- Botnets using encrypted communications
- Attacks against government infrastructure for political purposes
- Use of DoS by organised crime
- Attacks against virtual servers
- Increasing sophistication of malware and malware packaging

Future:

- Attacks on emerging technologies
- Application layer DoS
- Realistic behaviour of DoS traffic (further difficulty in detection)
- Attacks against anti-DoS infrastructure
- Attacks against SCADA systems
- Attacks against shared infrastructure and the 'cloud'
- Attacks against web services

Case Study: Major Australian ISPs subjected to DDoS Attacks

What happened?
In late 2009, two prominent Australian ISPs, aaNet and EFTel, were reportedly subjected to sustained DDoS attacks for a number of weeks. This severely inhibited their ability to provide quality service to customers due to a significant increase in packet loss and network latency.

The source of the attacks was initially unable to be pinpointed. Despite the longevity of the attacks, it is not clear whether the ISPs chose to contact law enforcement authorities for assistance.

Nevertheless, the attacks confirmed that Australian organisations with a reliance on the Internet are a legitimate target for DoS attacks and need to take appropriate precautions to deal with the threat posed by such attacks.

What was the impact?
It was reported that for several weeks the customers of both ISPs experienced significant deterioration in the quality of their service. The attacks received significant publicity in the media and resulted in several complaints from customers.

How was the situation handled?
The ISPs embarked upon a series of core network upgrades, including installing additional equipment to alleviate the attacks and provide additional capacity to their customer base.

In addition, the ISPs contacted their upstream providers and worked with them to implement filtering mechanisms to block the hosts identified as playing a key role in the attacks.

The initial effectiveness of the attacks, however, highlights the importance of Australian organisations proactively implementing a management framework to address the threat of DoS attacks.

Sources & Further information:
http://www.infosecurity-magazine.com/view/3371/australian-isps-tackling-ongoing-ddos-attack/
http://www.itnews.com.au/News/153241,eftel-aanet-suffer-denial-of-service-attack.aspx
http://forums.whirlpool.net.au/forum-replies.cfm?t=1263410#r1

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.

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 with external service providers
- Participating in joint exercises
- Improving information sharing
- Obtaining insurance
- Encouraging industry / government collaboration (examples include the Cyberstorm and Cyberstorm II security exercises)

At operational and technical levels, a range of actions can be taken to protect against attacks, detect attacks, and provide a structured and effective response.

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 help protect an organisation from DoS attacks:

- Conducting technology risk assessments considering the key variables discussed in this paper in the Risk Identification section
- Capacity planning
- Ensuring secure network design
- Ensuring physical security
- Utilising secure application design
- Including DoS in business continuity management
- 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
- Performing system hardening
- System & network segregation

Detect

Given the range of attacks covered by the broad titles 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. Groups such as CERT Australia are in a good position to predict, trace, and even work to shut down immediate threats to Australian critical infrastructure. Security vendors, including anti-virus firms and consulting firms, can also provide valuable advice on industry trends and response approaches. For this reason, it is recommended strong relationships are 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
- Deploying honeypot 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. Having clear incident escalation thresholds and clear internal communication paths between business areas in an organisation were identified in the Cyber Storm II exercise as key methods for improving incident response.
- 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. As identified in the Cyber Storm II exercise, established relationships with key organisations facilitates rapid information sharing during a DoS attack, helping to maintain situational awareness and ensuring more effective incident response and recovery. Establishing these relationships proactively is crucial because it is difficult to create trusted relationships during the middle 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.

Available Resources

A considerable amount of work has been done in establishing strategies to cope with DoS and other malicious attacks. Following these established 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 27002 *Code of Practice for Information Security Management* (2005) outlines best practices for organisational protection of information resources. Aligning practices with these requirements will aid in the overall management of DoS threats.
- ISM *Australian Government Information Security Manual* (2009) provides policies and guidance to Australian Government agencies on how to protect their ICT systems.
- *ISP Voluntary Code of Practice for Industry Self-Regulation in the Area of e-Security* (2009) provides a code of conduct for Australian ISPs regarding the management of situations where subscribers have malware-infected computers that form part of botnets.

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?

The preparedness of an organisation for a DoS attack is dependent on the technical and operational measures it has in place. Ensuring trading partners are also prepared for the threat of DoS attacks is important as interruptions to their business can affect your organisation.

What systems, connections and applications are most at risk?

Identifying the infrastructure and applications considered most vulnerable to DoS attacks is an important part of the Threat Assessment process and will assist in deploying appropriate controls to protect, detect and respond to attacks against these components.

Do external services we utilise (such as cloud computing solutions) have appropriate strategies to reduce the threat of DoS attacks?

It is important to ensure prior to engaging service providers that they have strategies and controls in place to address the threat of DoS attacks.

Would our organisation benefit from participating in an industry-wide preparedness test?

Participation in industry-wide tests allows for identification of common issues and vulnerabilities across organisation and allows for information-sharing to occur regarding the management of DoS attacks.

What are our contingency plans in the event that service has been denied to us?

Having Business Continuity Plans in place to deal with situations where a DoS attack affects your organisation or an organisation with whom your business is closely linked will assist in minimising the impact(s) of such an attack

Questions you should ask

Which resources would be potential targets for attackers and where are they vulnerable to attack?

Identifying resources vulnerable to DoS attacks is an important step in determining where the deployment of technical and operational measures to manage the DoS threat should be focussed.

Do we have any virtualised systems that require additional strategies to be in place to protect against DoS attacks?

The increasing use of virtual systems means that the potential effect of a DoS attack can be increased, since a successful attack on the underlying server can affect many systems located on the same physical infrastructure.

How can we recognise a DoS attack and how effective would our response be?

An organisation's ability to effectively recognise and respond to DoS attacks will be significantly enhanced through implementing the technical and operational measures identified in this paper as part of the Protect, Detect and React triad.

Are our service providers well placed to manage the threat of a DoS attack?

Ensuring service providers have protective measures in place should they be subjected to a DoS attack (for example, having sufficient bandwidth capacity and being able to maintain continuity of critical services such as web and email) is an important component of ensuring an organisation can continue to function in the event of an attack.

Do our contracts with providers allow us to expand our resource usage if required?

The ability to increase the resources available to an organisation during a DoS attack can provide an important means of minimising the impact of the attack on the business.

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. 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.

Following the recommendations contained in this paper will provide your organisation with a solid base for minimising the impact of these potentially damaging attacks.

Summary of recommended actions

Strategic	• Incorporate DoS into risk-management program • Negotiate service-level agreements with suppliers for DoS protection and response levels • Consider running DoS scenarios to identify weaknesses (individually and also with business partners) • Participate in DoS information-sharing networks such as TISN, ITSEAG and CERT Australia

	Operational	**Technical**
Protect	• Include DoS security in testing scope (IT Security Manager) • Complete bottleneck analysis on finite network resources (Network Architect/System Administrator) • Include security in application and network design (Application/Network Architect) • Plan for capacity to endure DDoS attacks (Network Architect) • Implement appropriate physical security measures (IT Security Manager/Operation Manager) • 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) • Configure routers and network edge devices according to best practice (Network engineer / System administrator)
Detect	• Create strong relationships with anti-virus vendors to keep abreast of the latest techniques and potential attacks (IT Security Manager)	• Deploy intrusion detection systems (IT Security Manager/Incident Response Team) • Develop monitoring & logging mechanisms (IT Security Manager/System Administrator)
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)

The Trusted Information Sharing Network

Since 2005, the IT Security Expert Advisory Group (ITSEAG)[i] of the Trusted Information Sharing Network (TISN)[ii] has released a series of papers designed to help CEOs, Boards of Directors and CIOs understand the threats to the information and IT infrastructure of their organisations and provide recommendations for mitigating those threats.

The papers cover many topical issues including information security governance, the strategy of defence in depth, managing denial of service attacks, effectively implementing user access management, and the security implications of technologies such as global positioning systems, Voice over IP, mobile devices and wireless networking.

Further information, reports and resources are available at the TISN website (www.tisn.gov.au).

The Australian Government provides support to critical infrastructure organisations in maintaining a secure IT environment. Services and support available include:

- Trusted Information Sharing Network (TISN)
  http://www.tisn.gov.au/
- SCADA Community of Interest
  Secretariat - scada@dbcde.gov.au

CERT Australia

*To enhance A*ustralia's cyber security capability, the Australian Government announced in May 2009 that it would create CERT Australia, the new national computer emergency response team. CERT Australia will be managed by the Australian Government

CERT Australia will be a source of cyber security information for the Australian community and point of contact for Australia's international cyber security counterparts. It will also provide a trusted environment for information exchange between the Government and business on cyber security related issues.

CERT Australia will coordinate government and non-government cyber security efforts and have a coordination role in the event of a serious cyber event.

By facilitating the sharing of information between Australian Internet service providers (ISP), major corporations, anti-virus researchers and information technology security vendors, CERT Australia will provide the Australian community with relevant and timely information on cyber security issues.

CERT Australia will incorporate a number of cyber security activities currently undertaken by Australian Government agencies, including the Australian Government Computer Emergency Readiness Team (GovCERT.au). It will also complement the work undertaken by the Cyber Security Operations Centre (CSOC), recently established in the Defence Signals Directorate, and help inform the Australian Government about the national cyber threat picture.

Contact details:

Website: www.cert.gov.au

Email: info@cert.gov.au

---

[i] The ITSEAG is one of three Expert Advisory Groups established within the Trusted Sharing Information Network for Critical Infrastructure Protection. The ITSEAG provides advice to the Critical Infrastructure Advisory Council (CIAC) and the sector based Information Assurance Advisory Groups on IT security issues as they relate to critical infrastructure protection. The ITSEAG membership consists of academic specialists, vendors, consultants and some industry association representatives who are leaders in the information technology/e-security fields.

[ii] 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, three Expert Advisory Groups, 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 or by contacting cip@ag.gov.au

End of Document