

Global Incident Analysis Center
- Special Notice -
© 1999 - 2000 SANS Institute

Consensus Roadmap for Defeating Distributed Denial of Service Attacks

A Project of the Partnership for Critical Infrastructure Security
Version 1.10 - February 23, 2000**

Prepared for the Partnership By:

CERT/CC at Carnegie Mellon University (Rich Pethia*),
The SANS Institute (Alan Paller*), and
The Center for Education & Research in Information Assurance & Security (CERIAS) at Purdue University (Gene Spafford*)

Reflecting the active participation, shared experience and insights of:

Stephen Northcutt of the Global Incident Analysis Center
Bill Cheswick of Lucent Technologies
Steve Kent* of BBN Technologies
Kelly Cooper from GTE Internetworking
Randy Marchany, Phil Benchoff, Valdis Kletnieks and Ron Jarrell of Virginia Tech University CIRT
David Dittrich of the University of Washington
Mudge* of The L0pht and @Stake
Neal Ziring of the National Security Agency
Eric Cole of Vista IT
Gary Gagnon, Steven Christey, and David Mann of MITRE
Andre Frech of Internet Security Systems
Kevin Ziese of Cisco
David LeBlanc of Microsoft
Craig Ozancin of Axent
Adam Shostack of BindView
Diego Zamboni, Tom Daniels and Pascal Meunier of Purdue University
Henry Kluepfel of SAIC

---

* Participants in the meeting on cybersecurity with President Clinton on February 15.
** This document is being updated. Before implementing the recommendations, email info@sans.org with the subject Roadmap. The latest version will be emailed to you.

Defeating Distributed Denial of Service Attacks
Version 1.10 February 23, 2000

Contents

1. Introduction
2. Key Trends and Factors
3. Immediate Steps To Reduce Risk and Dampen The Effects of Attacks
4. Longer Term Efforts to Provide Adequate Safeguards
5. A Living Document
6. Download this Document in MS Word format

Introduction

The distributed denial of service attacks during the week of February 7 highlighted security

weaknesses in hosts and software used in the Internet that put electronic commerce at risk. These attacks also illuminated several recent trends and served as a warning for the kinds of high-impact attacks that we may see in the near future. This document outlines key trends and other factors that have exacerbated these Internet security problems, summarizes near-term activities that can be taken to help reduce the threat, and suggests research and development directions that will be required to manage the emerging risks and keep them within more tolerable bounds. For the problems described, activities are listed for user organizations, Internet service providers, network manufacturers, and system software providers.

Key Trends and Factors

The recent attacks against e-commerce sites demonstrate the opportunities that attackers now have because of several Internet trends and related factors:

- Attack technology is developing in an open-source environment and is evolving rapidly. Technology producers, system administrators, and users are improving their ability to react to emerging problems, but they are behind and significant damage to systems and infrastructure can occur before effective defenses can be implemented. As long as defensive strategies are reactionary, this situation will worsen.

- Currently, there are tens of thousands – perhaps even millions – of systems with weak security connected to the Internet. Attackers are (and will) compromising these machines and building attack networks. Attack technology takes advantage of the power of the Internet to exploit its own weaknesses and overcome defenses.

- Increasingly complex software is being written by programmers who have no training in writing secure code and are working in organizations that sacrifice the safety of their clients for speed to market. This complex software is then being deployed in security-critical environments and applications, to the detriment of all users.

- User demand for new software features instead of safety, coupled with industry response to that demand, has resulted in software that is increasingly supportive of subversion, computer viruses, data theft, and other malicious acts.

- Because of the scope and variety of the Internet, changing any particular piece of technology usually cannot eliminate newly emerging problems; broad community action is required. While point solutions can help dampen the effects of attacks, robust solutions will come only with concentrated effort over several years.

- The explosion in use of the Internet is straining our scarce technical talent. The average level of system administrator technical competence has decreased dramatically in the last 5 years as non-technical people are pressed into service as system administrators. Additionally, there has been little organized support of higher education programs that can train and produce new scientists and educators with meaningful experience and expertise in this emerging discipline.

- The evolution of attack technology and the deployment of attack tools transcend geography and national boundaries. Solutions must be international in scope.

- The difficulty of criminal investigation of cybercrime coupled with the complexity of international law mean that successful apprehension and prosecution of computer crime is

unlikely, and thus little deterrent value is realized.

- The number of directly connected homes, schools, libraries and other venues without trained system administration and security staff is rapidly increasing. These "always-on, rarely-protected" systems allow attackers to continue to add new systems to their arsenal of captured weapons.

Immediate Steps to Reduce Risk And Dampen the Effects of Attacks

There are several steps that can be taken immediately by user organizations, Internet service providers, network manufacturers, and system software providers to reduce risk and decrease the impact of attacks. We hope that major users, including the governments (around the world) will lead the user community by setting examples – taking the necessary steps to protect their computers. And we hope that industry and government will cooperate to educate the community of users – about threats and potential courses of action – through public information campaigns and technical education programs.

In all of these recommendations, there may be instances where some steps are not feasible, but these will be rare and requests for waivers within organizations should be granted only on the basis of substantive proof validated by independent security experts.

Problem 1: Spoofing

Attackers often hide the identity of machines used to carry out an attack by falsifying the source address of the network communication. This makes it more difficult to identity the sources of attack traffic and sometimes shifts attention onto innocent third parties. Limiting the ability of an attacker to spoof IP source addresses will not stop attacks, but will dramatically shorten the time needed to trace an attack back to its origins.

Solutions:

- User organizations and Internet service providers can ensure that traffic exiting an organization's site, or entering an ISP's network from a site, carries a source address consistent with the set of addresses for that site. Although this would still allow addresses to be spoofed within a site, it would allow tracing of attack traffic to the site from which it emanated, substantially assisting in the process of locating and isolating attacks traffic sources. Specifically user organizations should ensure that all packets leaving their sites carry source addresses within the address range of those sites. They should also ensure that no traffic from "unroutable addresses" listed in RFC 1918 are sent from their sites. This activity is often called *egress filtering*. User organizations should take the lead in stopping this traffic because they have the capacity on their routers to handle the load. ISPs can provide backup to pick up spoofed traffic that is not caught by user filters. ISPs may also be able to stop spoofing by accepting traffic (and passing it along) only if it comes from authorized sources. This activity is often called *ingress filtering*.

- Dial-up users are the source of some attacks. Stopping spoofing by these users is also an important step. ISPs, universities, libraries and others that serve dial-up users should ensure that proper filters are in place to prevent dial-up connections from using spoofed addresses. Network equipment vendors should ensure that no-IP-spoofing is a user setting, and the default setting, on their dial-up equipment.

Problem 2: Broadcast Amplification

In a common attack, the malicious user generates packets with a source address of the site he wishes to attack (site A) (using spoofing as described in problem 1) and then sends a series of network packets to an organization with lots of computers (Site B), using an address that broadcasts the packets to every machine at site B. Unless precautions have been taken, every machine at Site B will respond to the packets and send data to the organization (Site A) that was the target of the attack. The target will be flooded and people at Site A may blame the people at Site B. Attacks of this type often are referred to as Smurf attacks. In addition, the echo and chargen services can be used to create oscillation attacks similar in effect to Smurf.

Solutions:

- Unless an organization is aware of a legitimate need to support broadcast or multicast traffic within its environment, the forwarding of directed broadcasts should be turned off. Even when broadcast applications are legitimate, an organization should block certain types of traffic sent to "broadcast" addresses (e.g., ICMP Echo Reply) messages so that its systems cannot be used to effect these Smurf attacks.

- Network hardware vendors should ensure that routers can turn off the forwarding of IP directed broadcast packets as described in RFC 2644 and that this is the default configuration of every router.

- Users should turn off echo and chargen services unless they have a specific need for those services. (This is good advice, in general, for all network services – they should be disabled unless known to be needed.)

Problem 3: Lack of Appropriate Response To Attacks

Many organizations do not respond to complaints of attacks originating from their sites or to attacks against their sites, or respond in a haphazard manner. This makes containment and eradication of attacks difficult. Further, many organizations fail to share information about attacks, giving the attacker community the advantage of better intelligence sharing.

Solutions:

- User organizations should establish incident response policies and teams with clearly defined responsibilities and procedures.

- ISPs should establish methods of responding quickly and staffing to support those methods when their systems are found to have been used for attacks on other organizations.

- User organizations should encourage system administrators to participate in industry-wide early warning systems, where their corporate identities can be protected (if necessary), to counter rapid dissemination of information among the attack community.

- Attacks and system flaws should be reported to appropriate authorities (e.g., vendors, response teams) so that the information can be applied to defenses for other users.

Problem 4. Unprotected Computers

Many computers are vulnerable to take-over for distributed denial of service attacks because of inadequate implementation of well-known "best practices." When those computers are used in attacks, the carelessness of their owners is instantly converted to major costs, headaches, and

embarrassment for the owners of computers being attacked. Furthermore, once a computer has been compromised, the data may be copied, altered or destroyed, programs changed, and the system disabled.

Solutions:

- User organizations should check their systems periodically to determine whether they have had malicious software installed, including DDOS Trojan Horse programs. If such software is found, the system should be restored to a known good state.

- User organizations should reduce the vulnerability of their systems by installing firewalls with rule sets that tightly limit transmission across the site's periphery (e.g. deny traffic, both incoming and outgoing, unless given specific instructions to allow it).

- All machines, routers, and other Internet-accessible equipment should be periodically checked to verify that all recommended security patches have been installed.

- The security community should maintain and publicize a current "Top-20 Exploited vulnerabilities" and the "Top 20 Attacks" list of currently most-often-exploited vulnerabilities to help system administrators set priorities.

- Users should turn off services that are not required and limit access to vulnerable management services (e.g., RPC-based services).

- Users and vendors should cooperate to create "system-hardening" scripts that can be used by less sophisticated users to close known holes and tighten settings to make their systems more secure. Users should employ these tools when they are available.

- System software vendors should ship systems where security defaults are set to the highest level of security rather than the lowest level of security. These "secure out-of –the-box" configurations will greatly aid novice users and system administrators. They will furthermore save critically-scarce time for even the most experienced security professionals.

- System administrators should deploy "best practice" tools including firewalls (as described above), intrusion detection systems, virus detection software, and software to detect unauthorized changes to files. This will reduce the risk that systems are compromised and used as a base for launching attacks. It will increase confidence in the correct functioning of the systems. Use of software to detect unauthorized changes may also be helpful in restoring compromised systems to normal function.

- System and network administrators should be given time and support for training and enhancement of their skills. System administrators and auditors should be periodically certified to verify that their security knowledge and skills are current.

Longer Term Efforts to Provide Adequate Safeguards

The steps listed above are needed now to allow us to begin to move away from the extremely vulnerable state we are in. While these steps will help, they will not adequately reduce the risk given the trends listed above. These trends hint at new security requirements that will only be met if information technology and community attitudes about the Internet are changed in fundamental

ways. In addition, research is needed in the areas of policy and law to enable us to deal with aspects of the problem that technology improvements will not be able to address by themselves. The following are some of the items that should be considered:

- Establish load and traffic volume monitoring at ISPs to provide early warning of attacks.
- Accelerate the adoption of the IPsec components of Internet Protocol Version 6 and Secure Domain Name System.
- Increase the emphasis on security in the research and development of Internet II.
- Support the development of tools that automatically generate router access control lists for firewall and router policy.
- Encourage the development of software and hardware that is engineered for safety with possibly vulnerable settings and services turned off, and encourage vendors to automate security updating for their clients.
- Sponsor research in network protocols and infrastructure to implement real-time flow analysis and flow control.
- Encourage wider adoption of routers and switches that can perform sophisticated filtering with minimal performance degradation.
- Sponsor continuing topological studies of the Internet to understand the nature of "choke points."
- Test deployment and continue research in anomaly-based, and other forms of intrusion detection
- Support community-wide consensus of uniform security policies to protect systems and to outline security responsibilities of network operators, Internet service providers, and Internet users.
- Encourage development and deployment of a secure communications infrastructure that can be used by network operators and Internet service providers to enable real-time collaboration when dealing with attacks.
- Sponsor research and development leading to safer operating systems that are also easier to maintain and manage.
- Sponsor research into survivable systems that are better able to resist, recognize, and recover from attacks while still providing critical functionality.
- Sponsor research into better forensic tools and methods to trace and apprehend malicious users without forcing the adoption of privacy-invading monitoring.
- Provide meaningful infrastructure support for centers of excellence in information security education and research to produce a new generation of leaders in the field.

- Consider changes in government procurement policy to emphasize security and safety rather than simply cost when acquiring information systems, and to hold managers accountable for poor security.

A Living Document

This Roadmap is a living document and will be updated periodically when new or altered threats require changes to the document. Furthermore it is a consensus document – a product of the joint thinking of some of the best minds in security – and it will continue to improve if you share your experiences in implementing the prescriptions.

© 1999 SANS Institute : **Office** 301.951.0102 : **Registration** 719.599.4303 : **Web Contact** scott@sans.org