Recent Developments and Emerging Defenses to D/DoS: The Microsoft Attacks and Distributed Network Security

Jay L. Koh
February 9, 2001

In recent months, a variety of new developments have occurred in the world of denial of service (DoS) and distributed denial of service (DDoS) attacks. This short paper discusses two phenomena in the area: (1) the recent Microsoft DoS attacks; and (2) emerging backbone-level defenses to DDoS attacks. DoS and DDoS have been discussed in depth elsewhere [1]; this paper assumes a general level of familiarity with the DoS and DDoS phenomena and supplements rather than reviews other discussions of the topic.

0. General Background

A denial of service (DoS) attack occurs when an attacker essentially floods a target or victim node with spurious or malformed packets, causing the node to crash or otherwise cease to function correctly. A variety of DoS attack techniques have been identified (including ICMP flood, SYN flood, UDP flood, and SMURF) targeted primarily at web servers or application servers with Internet access. [2]

As discussed elsewhere, distributed denial of service attacks (DDoS) are a variant of Denial of Service attacks (DoS), where attacks are launched from a number of nodes across the Internet as opposed to a single node or concentrated groups of nodes. An intruder takes over a first computer (called the master or handler) which then compromises and then installs a daemon (or agent or zombie) onto a number of other computers. At the intruder’s subsequent command, the master sends a command to the compromised computers, and the daemons on them launch denial of service attacks at the target victim computer. [3] A variety of different DDoS attacks have also been identified. [4]

1. A New Target: The Microsoft Attacks

The landscape of DoS attacks has apparently changed abruptly in January 2001, with the first high profile DoS attacks on network infrastructure devices: the DoS outages at Microsoft’s sites between January 25-26, 2001. Little information has been released about these attacks, which remain under investigation by Microsoft and the U.S. government. [5] This section discusses what is known about the attacks and provides the author's speculation as to what vulnerabilities might exist in similar systems.

a. Chronology

The company experienced three separate outages of its websites in late January 2001. First, Microsoft reported a 22.5-hour outage of its websites that ended on Wednesday evening, January 24, 2001. [6] It claims that this problem was not related to attacks on the company, but rather to a misconfiguration of its Domain Name System (DNS) servers by one of its technicians. (DNS is a database system that matches the more easily remembered Universal Resource Locators (URLs or domain names) with the IP addresses of particular devices. [7] Because DNS servers provide this name matching function, subverting or crashing these servers can misdirect, slow or halt Internet traffic.)

Second, on the morning of Thursday, January 25, 2001, Internet users attempting to connect to Microsoft's sites experienced a denial of service. Expedia.com and MSN.com began experiencing significant reductions in availability of service beginning in the early morning, with normal connection success rates of about 97 percent plummetting to 70, 55 and eventually 1.5 percent, according to Keynote Systems, a performance benchmarking company. [8] Performance fluctuated throughtout the day, finally recovering by late afternoon.

Third, on the morning of Friday, January 26, 2001, Microsoft again experienced a successful DoS attack. [9] The company reported that the attack was similar to second, and that it caused two 15-minute service outages.

b. Description

Although little is known about the attacks, the following details have been released:

First, the Microsoft attacks appear to have been been directed at the company's routers, specifically its Domain Name Service (DNS) servers. By contrast, previous DoS attacks aimed at web or application servers. This new DNS-flooding attack is more complex than other well-known DoS or DDoS attacks that have been in the news lately and for which pre-written code exists and is commonly available over the Internet. [10].

Second, unlike previously known attacks on DNS servers (which poison the DNS address database, misdirecting traffic, or subvert the DNS operating system know as BIND [11]), the attacks appear to have simply shut or slowed down the performance of the DNS servers. Microsoft has characterized the denials of service as resulting from "someone attempt[ing] to block legitimate access to our Web properties by flooding our network routers with large volumes of bogus requests." [12] Although the type of attack used is not entirely clear, this description seems quite different from other DNS attacks.

c. Analysis

The Microsoft attacks suggest three observations. First, DNS servers are important and their software is vulnerable. Over the last few months, CERT has continued to review and reveal vulnerabilities in earlier versions of BIND, the operating software for DNS servers. [13]. Many of these vulnerabilities enable attackers to take over DNS servers or to cause denial of service problems by forcing them to reboot or by forcing them to engage in additional complex computations. Specific Denial-of-Service attacks on BIND have been identified. [14] It is not yet clear which, if any, of these attacks were launched against Microsoft's DNS servers, or if an entirely new attack was used. What is clear is that high profile DNS attacks have now occurred, can be expected to become more common, and can be quite effective, given existing vulnerabilities.

Second, DNS network architecture matters. Microsoft's first outage and the pattern of the two successful DoS attacks have led security experts to speculate that one major vulnerability of Microsoft's DNS servers was that they may have been placed on a single part of the network and were not backed-up or distributed. [15] The fact that a DNS configuration error led to the first 22.5 hour outage suggests that a single point of failure existed in the Microsoft DNS architecture. The effectiveness of the two admitted DoS attacks also supports the likelihood of this potential vulnerability. Finally, the fact that immediately following the second attacks, Microsoft contracted with Akamai to operate backup DNS servers, which could provide DNS routing if Microsoft's DNS servers went down. [16]

Third, revealing information about the vulnerability of a network matters. Several security commentators have suggested that Microsoft’s first 22.5 hour outage revealed its vulnerability to a DNS attack.[17] Moreover, CERT’s recent focus on BIND vulnerability in the DNS system within such a short time of the attacks on Microsoft’s DNS servers seems to be too close in time to be a simple coincidence.

d. Recommendations

Given these observations, to increase the security of their DNS servers against DoS attacks, information security officers should:

1. Update and maintain the current build of BIND software on their DNS servers;
2. Carefully architect their DNS server network, distributing DNS servers around the edge of the corporate network and consider establishing back-up relationships with other parties;
3. Safeguard information about the architecture and thus vulnerability of DNS networks.

2. Distributed Network Security

A second important recent development in the DoS/DDoS security arena has been the emergence of a distributed network approach to security.

a. The Problem

Because of the distributed nature of DDoS attacks, it is very difficult to track down the actual intruder and also quite difficult to stop the attack. To date, most of the DoS and DDoS countermeasures have also focused solely on the enterprise itself at the firewall or router level. The problem is that although these measures can safeguard the web servers within the enterprises from being compromised or crashed by intelligently dropping packets or blocking connections, legitimate traffic to the site under attack can still be crowded out by the flood of illegitimate traffic. Moreover, as the Microsoft incident appears to suggest, attacks on unsecured routers a step or more back into the backbone from the enterprise can cause DoS effects even if the enterprise uses existing countermeasures to protect its own assets.

b. A Proposed Solution

One recently proposed approach to solving this problem has been to detect and choke off illegitimate flooding traffic generated by DDoS or DoS attacks earlier in the path of transmission to the site, i.e., shutting down or dropping bogus packets at a router nearer to the source of the attacks. In addition to the technical difficulty of tracing patterns of traffic backwards into the core of the network and beyond, such an effort requires the coordination of multiple and interconnecting backbone networks owners over whose networks these attacks are being launched and in whose networks they must be tracked and stopped to prevent effective DoS by crowding out legitimate traffic, if not crashing the target server, as well as the enterprises who are the ultimate targets. ISPs, hosting companies, and carriers own and control the infrastructure where such attacks might be detectable and stopped prior to impacting the enterprise itself, but at present have little incentive of open their networks to security management software which directly benefits (for now) only the targeted enterprise.

c. Recent Developments

Although merely mentioned as a possibilty in discussions of DDoS last year [18], the intelligent network management/backbone-layer security approach appears to be under rapid development right now. Three companies have announced products aimed at stopping DDoS attacks before they reach the enterprise firewall: Most early announced were Asta Networks in Seattle, Washington [19], and Mazu Networks in Boston, Massachusetts [20]. A third company, Arbor Networks in Waltham, Massachusetts [21], has also recently announced its formation.

All three companies appear to take a similar approach, analyzing the patterns of traffic through the routers at the core and edge of the network, determining whether anomalies in the traffic suggests an attack on a router, server, or other piece of infrastructure is underway, tracing the attack back through the router system if an attack is detected, and the ultimately employing countermeasures against the attack by intelligently dropping packets or throttling back traffic over certain routers. [22]. Whether these solutions create a software overlay on top of existing router networks, develop and add additional hardware to the system, or require new equipment is not yet entirely clear.

To date, the distributed network security approach has made considerable progress. From the formation of these companies within the last year, two have been testing their ability to detect, trace, and push back simulated DDoS attacks at Exodus [23], and one has been installed in a small part of the academic Internet 2 project, where it has detected a number of live DDoS attacks [24].

As noted above, implementing this kind of distributed approach to detecting and pushing back DDoS attacks would require considerable coordination among the different owners of the networks and routers over which illegimate traffic might pass. Moreover, the ability to engage in such security without significantly degrading the performance of the networks also remains in serious question. Furthermore, how the ultimate target enterprise persuades carriers to implement this solution is also unclear, although attacks on routers rather than servers might create incentives for network operators to adopt this solution.

3. Conclusion

In sum, DoS and DDoS attacks continue to develop and evolve. The latest, the Microsoft attacks on a network infrastructure router (the DNS server), reveals both a new set of threats to the security of the overall network and points out specific means in which existing networks can be strengthened and made less vulnerable (e.g., creating backup DNS servers, distributing them across more than one localized area of a network, updating and maintaining the proper operation software). At the same time, new distributed defenses to these kinds of attack continue to evolve as well, with at least three companies developing a distributed solution that if adopted by the required carriers, could solve the effect of the DoS or DDoS problem earlier in the network. Both developments should be watched with some care.

[1] For a general discussion of DoS, see Fuller, Edward R. "Denial of Service Attack." 6 Apr. 2000. URL: http://www.sans.org/infosecFAQ/securitybasics/dos.htm (9 Feb. 2001). For a similar discussion of DDoS, see Kessler,

Gary C. “Defenses Against Distributed Denial of Service Attacks.” 29 Nov. 2000. URL: http://www.sans.org/infosecFAQ/threats/DDoS.htm (9 Feb 2001). See also National Infrastructure Protection Center. “Advisory 00-063 New Year’s DDOS Advisory.” 28 Dec. 2000. URL: http://www/nipc.gov/warnings/advisories/2000/00-063.htm (9 Feb. 2001).

[2] See Seifried, Kurt. “Denial of Service (DoS) FAQ.” 5 Mar. 2000. URL: http://securityportal.com/research/ddosfaq/html (9 Feb. 2001). For more recent developments, see, e.g., CERT/CC. “CERT Advisory CA-1999-17 Denial-of-Service Tools.” 3 Mar. 2000 (update). URL: http://www.cert.org/advisories/CA-1999-17.html (9 Feb. 2001); CERT/CC and FedCIRC. “CERT Advisory CA-2000-01 Denial-of-Service Developments.” 3 Jan. 2000. URL: http://www.cert.org/advisories/CA-2000-01.html (9 Feb. 2001); Copans, Brandi. “NAPTHA: A new type of Denial of Service Attack.” 10 Dec. 2000. URL: http://www.sans.org/infosecFAQ/threats/naptha2.htm (9 Feb. 2001).

[3] See Kessler [1].

[4] See Kessler [1]. More recent DDoS attacks are described in Sheridan, David. “Trinity v3 DDoS: Tomorrow’s Headline?” 19 Sept. 2000. URL: http://www.sans.org/infosecFAQ/malicious/trinity_ddos.htm (9 Feb. 2001); and Boyle, Phillip. “Distributed Denial of Service Attack Tools: trinoo and wintrinoo.” URL: http://www.sans.org/newlook/resources/IDFAQ/trinoo.htm (9 Feb. 2001).

[5] Fisher, Dennis & Callaghan, Dennis. “Microsoft attack raises concern over new DDOS variant.” 26 Jan. 2001. URL: http://www.zdnet.com/eweek/stories/general/0,11011,2679094,00.html (9 Feb. 2001).

[6] Devenuti, Rick. “Microsoft Explains Site Access Issues.” 25 Jan. 2001. URL: http:www.microsoft.com/info/siteaccess.htm (9 Feb. 2001).

[7] See Hanley, Sinead. “DNS Overview with a discussion of DNS Spoofing.” 6 Nov. 2000. URL: http://www.sans.org/infosecFAQ/DNS/DNS.htm (9 Feb. 2001).

[8] Dudley, Brier. "More Microsoft Web woes; this time, it's hackers." 26 Jan. 2001. URL: http://seattletimes.nwsource.com/cgi-bin/WebObjects/SeattleTimes.woa/wa/gotoArticle?zsection_id=268466359&text_only=0&slug=microsoft26&document_id=134262903 (9 Feb. 2001); Lemos, Robert. "TGIF: Microsoft's week of Web woes finally at a close?" 26 Jan. 2001. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2679162,00.html (9 Feb. 2001);

[9] Devenuti, Rick. "Statement of Rick Devenuti, Vice President and Chief Information Officer of Microsoft Corp." 26 Jan. 2001. URL: http://www.microsoft.com/presspass/press/2001/Jan01/01-26DevenutiPR.asp (9 Feb. 2001).

[10] See Fisher & Callaghan [5].

[11] For a discussion of known DNS attacks, see Hanley [7].

[12] See Devenuti [9]; Babcock, Charles. "Microsoft Repels More Attacks." 29 Jan. 2001. URL: http://www.zdnet.com/intweek/stories/news/0,4164,2679418,00.html (9 Feb. 2001).

[13] See, e.g., CERT/CC. "CERT Advisory CA-1999-14 Multiple Vulnerabilities in BIND." 25 Apr. 2000 (revised). URL: http://www.cert.org/advisories/CA-1999-14.html (9 Feb. 2001); CERT/CC. "CERT Advisory CA-2001-02 Multiple Vulnerabilities in BIND." 2 Feb. 2001 (revised). URL: http://www.cert.org/advisories/CA-2001-02.html (9 Feb. 2001); CERT/CC. "CERT Advisory CA-2000-03 Continuing Compromises of DNS servers." 26 Apr. 2000 (revised). URL: http://www.cert.org/advisories/CA-2000-03.html (9 Feb. 2001) .

[14] CERT/CC. "CERT Advisory CA-2000-20 Multiple Denial-of-Service Problems in ISC BIND." 28 Nov. 2000 (revised). URL: http://www.cert.org/advisories/CA-2000-20.html (9 Feb. 2001).

[15] Field, Ben. "Microsoft Notwork: The Anatomy of a DoS." 25 Jan. 2001. URL: http://www.securityportal.com/articles/microsoft20010125.html (9 Feb. 2001).

[16] Rowell, Erica D. “Technology’s Monday Morning Quarterback.” 29 Jan. 2001. URL: http://www.abcnews.go.com/sections/scitech/DailyNews/microsoft010129.html (9 Feb. 2001).

[17] See Fisher & Callaghan [5]; Rowell [16].

[18] See Kessler [1].

[19] http://www.astanetworks.com

[20] http://www.mazunetworks.com

[21] http:///www.arbornetworks.com

[22] Each of the companies has had its technology described in this general way. See Lawson, Stephen. “Asta Networks claims cure for DoS attacks.” 17 Jan. 2001. URL: http://www.infoworld.com/articles/hn/xml/01/01/17/010117hnasta.xml (9 Feb. 2001); Mazu Networks. “The denial-of-service problem.” URL: http://www.mazunetworks.com/white/dos/html (9 Feb. 2001); “Arbor Networks Forms to Address Proliferating Availability Threats Faced By Web Content, Hosting Providers.” 5 Feb. 2001. URL: http://www.arbornetworks.com/news/pr/1.html (9 Feb. 2001).

[23] Frishberg, Manny. “A Star Wars Defense to Hackers.” 21 Nov. 2000. URL: http://www.wired.com/news/technology/0,1282,40297,00.html (9 Feb. 2001); Tadjer, Rivka. “Detect, Deflect, Destroy.” 13 Nov. 2000. URL: http://www.internetweek.com/indepth/indepth111300.htm (9 Feb. 2001).

[24] “Asta Networks Deploys Technology in Internet2 Network to Protect Nationwide Backbone From Denial of Service Attacks.” 20 Nov. 2000. URL: http://www.astanetworks.com/News/pr02.htm (9 Feb. 2001).