Global Information Assurance Certification Paper

DNS Vulnerabilities – Nine Days in the Spotlight

By Cheryl Culpepper Olusada

February 15, 2001

The Domain Name System (DNS) is a distributed database used by TCP/IP applications to map between hostnames and IP addresses, and to provide electronic mail routing information. DNS is a critical component of web browsing. It allows users to connect to servers via alpha characters rather than the numeric IP address. Client machines access DNS through a resolver. The resolver gets the hostname and returns the IP address or gets an IP address and looks up a hostname. This process is known as a DNS query. (1)

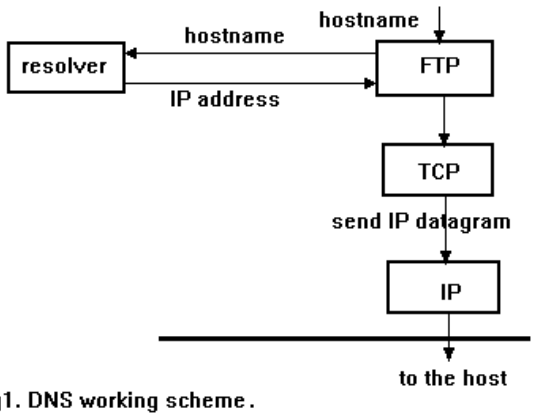

Fig1. DNS working scheme.

The distributed database contains "all" registered names organized into seven groups known as top-level domains. These generic domains are .com, .org, .edu, .net, .int, .gov and .mil. In addition there are two-letter "country code" domains. Each generic domain has a root name server which points to the authoritative name servers of each second-level domain or zone. The second-level name servers point to the sub-domain servers.

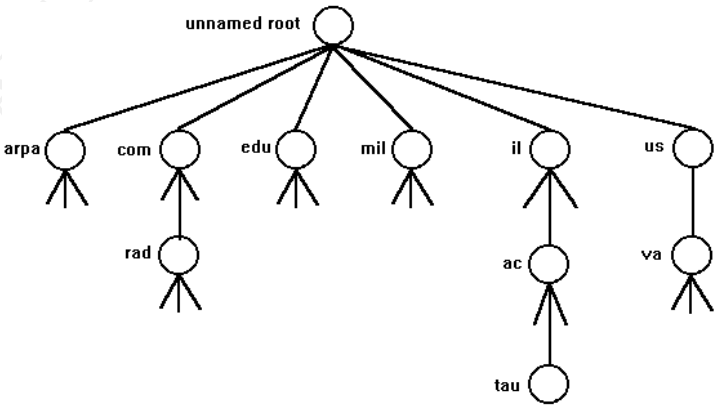

Fig.2 Hierachical organization of the DNS .

Each name server is not actually a single server but a group of two or more machines, one is designated as the primary (authoritative) and the others are secondary (cache). Caching is a fundamental property of DNS it provides redundancy and optimizes searches.

On the surface the role of DNS seems simple, sort of a huge HOSTS file accessible by everyone. However implicit in the "publicness" of DNS is a security risk. DNS was designed to be user friendly, you provide the site name, it finds the correct computer. Security concerns were an afterthought. RFC 2065 – Domain Name System Security Extensions states in the Abstract that "The Domain Name System (DNS) has become a critical operational part of the Internet infrastructure yet it has no strong security mechanisms to assure data integrity or authentication." The document recommends use of "extensions to the DNS that provide these services to security aware resolvers or applications through the use of cryptographic digital signatures." However section 2.1 states "It is part of the design philosophy of the DNS that the data in it is public and that the DNS gives the same answers to all inquirers. Following this philosophy, no attempt has been made to include any sort of access control lists or other means to differentiate inquirers. In addition, no effort has been made to provide for any confidentiality for queries or responses." (2) So attempts are being made to somewhat secure DNS, but the philosophy of open access remains. Security sites report that on a daily basis small sites go down because of vulnerabilities in the Internets addressing system. These problems with the domain name servers could be caused by something as simple as a single miss-typed number or letter in a piece of software. That's because the Internet was set up on the philosophy that the survival of the network as a whole is more important than that of an individual site or group of sites. (3)

During the period between January 21 and January 29, 2001 the vulnerabilities of DNS were exposed in a very public way. DNS was disrupted by a spoofing incident that resulted in domain hijacking. Serious problems with network design; configuration management and a poor disaster recovery plan took a second level DNS server offline making several major sites unreachable. And finally hackers launched a new variation of a distributed denial of service attack (DDoS).

January 21 and 22, 2001: A web hosting company, MyDomains.com released a DNS table that redirected web traffic from Yahoo.com to a page inside MyDomains.com. In addition other sites including Microsoft.com, MSN.com and several .net sites were also redirected to MyDomains.com. Over 100,000 Internet users were affected by the glitch which continued almost 24 hours. Richard Lau, president of the company said, "The episode proves a computer criminal could easily hijack all traffic on a part of the Internet. Imagine if we were malicious . . .It doesn't take much for a 16-year old to set up a name server. People could set up a name server . . . and hijack all traffic. It's mindboggling that ISPs out there have their systems misconfigured" (4)

Traditionally, domain hijackings happen when attackers block access to a legitimate DNS server and replace it with their own. This DNS incident was different because this was a data attack rather than a hardware attack. By altering data in key DNS tables users were

redirected just as successfully as implementing a rogue DNS server. Security analysts have said that MyDomains.com may not have been entirely innocent in this incident. The page that web surfers inadvertently reached was full of pay-per click links. MyDomains.com may have taken advantage of a well-known DNS vulnerability by actively presenting themselves as a name server authority to users. However the ISP involved also shoulders some blame because they are responsible for making sure known DNS holes are closed.

January 23, 2001: A Microsoft technician made a configuration change to two routers on the edge of the Microsoft DNS network. The change limited communication between DNS servers on the Internet and Microsoft's DNS servers. This limited communication caused many Microsoft sites to be unreachable. (5) The outage kept sites off line for 24 hours and affected millions of users. Ironically much of the problem could have been prevented, or at least corrected in a timely manner. According to Russ Cooper, Security Analyst there were several critical mistakes. " For a company the size of Microsoft there was no excuse for such a blunder. Clearly there is no system of peer vetting or management sign-off regarding production changes. Why didn't the DNS section of their disaster recovery plan include checking the router configuration? Distributed design for such an important component should include multiple sites" (6)

This DNS incident is clearly the failure of Microsoft to implement a Defense in Depth security model. A key component of this model is that the loss or failure of a single component does not compromise the entire information infrastructure. Critical systems should be fault tolerant and have hot-standbys available. There should also be strong configuration management controls. Good configuration management practices will limit system changes that may trigger false alerts or failures. Each system needs established baseline standards. Documentation of initial configurations should be supplemented by a system that details all patches; updates and other modification made to each machine.

January 24 and 25, 2001: An unknown person or persons initiated a distributed denial-of-service attack against the routers in front of the Microsoft DNS network They flooded the routers with traffic and blocked legitimate users. Affected sites included microsoft.com, msnbc.com, msn.com, expedia.com, slate.com and hotmail.com. At the height of the attack as little as 2% of the web page requests were being completed. Normally, sites are able to fulfill 97% of requests. For about two hours the attack was 100% successful. . Previous DDoS attacks have targeted servers. However the attackers used information gained from the previous day's news reports, and Microsoft's domain registration records. This information confirmed that all the DNS servers were on a single subnet. The routers became a target because they were the single point of failure to the DNS network. Experts say that the incident could have been a distinct DoS attack. "This is definitely more difficult [than a DDoS attack] because there's not the huge laundry list of tools available to do it on the Web. It's the first example we've seen of an infrastructure attack, but you'll see more of them in the future. This type of hack is also more difficult to identify and defend against, because instead of receiving the tell-tale flood of packets and huge consumption of bandwidth that signal a DDoS attack, the target's Web servers operate normally during this kind of event. There are some attacks

that can cause a router to reboot, so you only need to send packets every five or six minutes to keep tacking it down."(7)

This attack was a direct result of the misconfigurations revealed in the January 23rd outage. "National or global organizations should, as standard operating procedure, have their DNS servers on different networks served by different ISPs and running on different operating systems – Solaris and FreeBSD, or Linux and HPUX – so as to minimize the threats for DoS attacks, known OS vulnerabilities, and connectivity issues." (8) Microsoft failed to follow its own recommendations concerning the management of DNS. Chapter 9, "Managing MS DNS Servers," of the Microsoft Windows NT Server 4.0 Networking Guide states: Generally, plan to install the primary and secondary servers on different subnets to provide continual support for DNS name queries if one subnet should go down. The minimum number of DNS servers needed to serve each zone is two – a primary and a secondary == to provide database redundancy. As with any fault tolerant system, the computers should be as independent as possible, for example, by placing the primary and secondary servers on different subnets. (9)

On January 29th Microsoft issued a statement that they had contracted with Akamai Technologies of Cambridge, Massachusetts to distribute its DNS systems. Akamai focuses on ways of eliminating Internet bottlenecks and speeding download times. They have placed hundreds of servers inside ISP networks, as close to end users as possible. Its infrastructure allows many surfers to download much of the page from computers geographically close to their own instead of from computers across the country, speeding download times. According to Microsoft CIO Rick Vevenuti "One of the fastest lessons learned from last week's problems was to go ahead and distribute our DNS systems over several locations. In the past, Microsoft has focused on understanding and protecting against attacks on Microsoft products. Unfortunately, as we have learned over the last few days, we did not apply sufficient self-defense techniques to our use of some third-party products at the front-end parts of our core network infrastructure."(10)

January 29, 2001: The Computer Emergency Response Team (CERT) issued an advisory, warning of four serious problems affecting DNS Servers running various versions of Internet Software Consortium (ISC) BIND (including both 4.9.x prior to 4.9.8 and 8.2.x prior to 8.2.3; 9.x is not affected) and derivatives. (11) Because the normal operation of most services on the Internet depends on the proper operation of DNS servers, other services could be impacted if these vulnerabilities are exploited. The majority of name servers in operation today run BIND; these vulnerabilities present a serious threat to the Internet infrastructure.

Since 1997, the CERT/CC has published twelve documents describing vulnerabilities or exploitation of vulnerabilities in BIND with information and advice on upgrading and preventing compromises. Unfortunately, many system and network administrators still have not upgraded their versions of BIND, making them susceptible to a number of vulnerabilities. Prior vulnerabilities in BIND have been widely exploited by intruders.
For example, on November 10, 1999, the CERT/CC published CA-1999-14, which detailed multiple vulnerabilities in BIND. The CERT/CC continued to receive reports of

compromises based on those vulnerabilities through December 2000. On April 8, 1998, the CERT/CC published CA-1998-05 a compilation of prior reports. Attacks on vulnerabilities reported in the advisory reached their maximum approximately two months after release of the advisory, indicating that intruders pay more attention to vulnerability information than do network administrators. Based on this past experience, the CERT/CC expects that intruders will quickly begin developing and using intruder tools to compromise machines. It is important for IT and security managers to ensure that their organizations are properly protected before the expected widespread exploitation happens.

Lessons Learned

DNS is a weak link in Internet infrastructure. It is hampered by a combination of lack of security in the initial DNS design philosophy, vulnerabilities in the most popular DNS service, and the failure of individual companies and ISP's to implement "best practices". However many large corporations worry about distribution of Web site content, and forget about DNS. DNS software and consultancy firm Men and Mice recently checked the sites of 978 of the Fortunes 1000 companies. 25% of them had a bad DNS configuration. Another survey of 5000 random sites in the .com domain showed that 38% had shaky DNS configurations. (12)

DNS is serving functions and protocols that it was never intended to be responsible for – load balancing, load sharing, and high-availability Web sites. Instead of going back and looking at DNS to see how we can re-engineer it, people are adding tricks to it to let them do what they want. Worse, if DNS starts fracturing under the stress, the whole Internet could be at risk. DNS itself is a single point of failure; everything else relies on it. If a mail server is down, that doesn't mean the Web is down. But if a DNS server is down, then your site is off the Internet. (13) Perhaps the time has come to look at DNS more closely. E-commerce is increasing becoming a bigger portion of the corporate bottom-line. The DNS of the Internets early days was appropriate for it's user base of academia and government researchers. However we are now in a new era where the Internet need to be driven by a higher set of security standards. DNS is too critical not to be protected from the unscrupulous.

Finally it is prudent for every IT manager to review the Ten Immutable Laws of Security Administration. (14)

Law #1: Nobody believes anything bad can happen to them, until it does
Law #2: Security only works if the secure way also happens to be the easy way
Law #3: If you don't keep up with security fixes, your network won't be yours for long
Law #4: It doesn't do much good to install security fixes on a computer that was never secured to begin with
Law #5: Eternal vigilance is the price of security
Law #6: There really is someone out there trying to guess your passwords
Law #7: The most secure network is a well-administered one
Law #8: The difficulty of defending a network is directly proportional to its complexity
Law #9: Security isn't about risk avoidance; it's about risk management
Law #10: Technology is not a panacea

Sources

1. Galperin, Meir., Gordin, Ira. *DNS: The Domain Name System* (Online, accessed 14, February 2001). Available: http://www.rad.com/networks/1995/dns/dns.htm
2. Eastlake, D., Kaufman, C. *Network Working Group, Request for Comments: 2065* (Online, accessed 29, January 2001). Available: http://www.ietf.org/rfc/rfc2065.txt?number=2065
3. Chaand, Ariana., Streitfeld, David. *Microsoft Sites Inaccessible* (Online, accessed 31 January 2001). Available: http://www.washingtonpost.com/ac2/wp-dyn/A43208-2001Jan24?language=printer
4. Sullivan, Bob. *Yahoo, Microsoft traffic 'hijacked"* (Online, accessed 25, January 2001). Available: http://www.msnbc.com/news/519306.asp
5. *Microsoft Explains Site Access Issues* (Online, accessed 25, January 2001). Available: http://www.microsoft.com/info/siteaccess.htm
6. Cooper, Russ. *NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM* (Online, received 25, January 2001)
7. Fisher, Dennis., Callaghan, Dennis. *Microsoft attack raises concern over new DDOS variant* (Online, accessed 6, February 2001). Available: http://www.zdnet.com/filters/printerfriendly/0,06061,2679094-2,00.html
8. McCullagh, Declan. *How, Why Microsoft Went Down* (Online, accessed 26, January 2001). Available: http://www.wirednews.com/news/technology/0,1282,41412,000.html
9. Domingo, Michael. *MCPMAG@101dommunications-news.com* (Online, received 1, February 2001)
10. Weiss, Todd R. *Microsoft admits defense against attacks was inadequate* (Online, accessed 8 February 2001) Available: http://www.computerworld.com/cwi/Printer_Friendly_Version/0,1212,NAV47_STO57054-,00
11. *CERT® Advisory CA-2001-02 Multiple Vulnerabilities in BIND* (Online, accessed 29, January 2001) Available: www.cert.org/advisories/CA-2001-02.html
12. Evers, Joris. *Survey: 25% of Fortune 1,000 has bad DNS* (Online, accessed 31 January 2001) Available: http://computerworld.com/cwi/Printer_Friendly_Version/0,1212,NAV47_NLTnw_STO570.75
13. Lemos, Robert. *Too many holes in the Net* (Online, accessed 6, February 2001) Available: http://www.zdnet.com/filters/printerfriendly/0,6061,2679081-2,00.html
14. Culp, Scott. *The Ten Immutable Laws of Security Administration* (Online, accessed 18, January 2001) Available: http://www.microsoft.com/technet/security/10salaws.asp?a=printable