Global Information Assurance Certification Paper

Current Issues in DNS Security: ICANN's November 2001 Annual Meeting
By James Sweetman

Abstract: After a brief, policy-level introduction to DNS and ICANN, this paper summarizes the results of a 4-day meeting held during November 2001 on DNS security issues. The discussions addressed three primary topics: existing DNS security measures, the security risks in the DNS and number management, and the responses by ICANN and the community.

Background: DNS and ICANN

The domain name system is critical to the smooth operation of the Internet. It links domain names like "thomas.loc.gov" with the underlying numerical addresses that computers use to communicate with each other, called IP addresses. Each computer on the Internet needs a unique IP address to distinguish it from other computers. For example, the IP address of the computer that hosts the Thomas system at the Library of Congress is 140.147.248.9. However, IP address can be hard for people to remember. Domain names were created in order to provide an easy to use substitute for IP addresses.

Domain names are organized into a hierarchy. The letters that appear at the far right of a domain name are called top-level domains (TLDs), and include a small number of generic names such as .com and .gov, as well as country-codes such as .us (United States) and .ca (Canada). The next string of text to the left ("loc" in the thomas.loc.gov example), is called a second-level domain, and is a subset of the top-level domain. Second-level domains, too, can be divided further. In our example, "thomas" is a third-level domain.

Each top-level domain had an administrator, or registry, responsible for assigning second-level domains within its branch, or domain. For most generic top-level domains, the registry has contracted with numerous registrars to perform name assignment at the retail level. Once a user is assigned a second-level domain, it is up to that user to configure the appropriate third- and lower-level domains for its network.

Computers translate names into address and back again in a process transparent to the end user. This process relies on a system of servers, collectively known as the domain name service (DNS), which store data linking names with numbers. Each domain name server stores a limited set of names and numbers. They are linked by a series of thirteen "root servers," which coordinate the data and allow users to find the server that identifies the site they want to reach. One of the root servers, designated the "authoritative root," maintains the master copy of the coordination file, called the root zone file. The other twelve servers maintain copies of the file provided by the authoritative root server, and make it available to the domain name servers. The domain name servers are organized into a hierarchy that parallels the organization of the domain names. Specifically, the 13 root servers maintain authoritative information about the top-level domains. In turn, each TLD provides authoritative domain name

information for the second-level domains in its zone, while those second-level domains provide domain name services for resources in their zones. [1]

Researchers funded by the U.S. Department of Defense developed DNS and the root server system. In the late 1990's the Clinton Administration issued a policy directive calling for the privatization of Internet management. In response, the Department of Commerce entered into a Memorandum of Understanding with the Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit corporation governed by a board of directors with broad international representation. The agreement with the government called on ICANN to design, develop, and test procedures for performing the coordinating functions previously performed by the government-funded researchers. These tasks included the allocation of IP numbers, the coordination of Internet protocols, and the management of the domain name system. ICANN and the Department were jointly tasked with conducting a study to suggest ways to improve the stability and security of the root server system. [2,3,4]

In response to the events of September 11, 2001, ICANN announced that it had changed the format for its annual meeting the following November. ICANN arranged for presentations on security from operators of various DNS services, as well as an open discussion on security vulnerabilities and ways to secure those vulnerabilities. The sections below summarize the discussions. [5]

Current Security Procedures

The root servers are the heart of the DNS. There are 13 servers in various locations in four countries (the U.S., U.K., Japan and Sweden), run by 10 separate organizations. According to the chairman of ICANN's root server study committee and the server operators themselves, the root servers employ a number of security features. First, the distributed nature of the servers offers redundancy and excess capacity. Several servers could go down with no impact on the Internet because the remaining servers could handle the traffic. The root servers also use various hardware and operating system configurations, thus limiting the damage that that could occur from a single vulnerability. Physical security includes limiting access to the facility where the server is located, and providing power backup and redundant communications channels. Some operate "hot spares" – systems that can be put into service immediately in case of emergency. Each server operator also has contingency plans for various types of situations. In a worst case scenario, one operator stated that service could be restored using a LINUX-based laptop in a couple of hours. [6,7}

The main job of the root servers is the storage and distribution of the zone file, or the master file that lists the name and address of each top-level domain. These files can be authenticated using cryptography. Protocol (scheduled) transfers under DNSsec have the option of using symmetrical key encryption (TSIG or transaction signature) to confirm the validity of the file. Zone files requested via e-mail require a public key-signed message (PGP). However, the DNSsec standard has not been finalized and not universally deployed. [8]

Top-level domain (TLD) registries described security precautions similar to those employed by the root servers. According to their presentations, the various TLD registries also employ multiple redundant connections, various hardware and software configurations, physical access control, and contingency planning. In addition, some registries noted that they use constant network monitoring and participation on various security lists to get advance warning of problems. Also, because TLD registries are constantly adding and deleting domain names from their databases, data integrity is more difficult than with the root servers. As a result, the registries put more effort into scrubbing data to ensure that it is consistent across the various databases and that improper data (such as identifying a bogus name server) are deleted promptly. [9,10]

Outstanding Security Issues

In the area of number allocation, inaccurate data on IP address ownership is a risk area. Without accurate information on who owns each address, it is difficult to track down bad actors. However, while the data on newer addresses is pretty good, data on older blocks is often outdated. For example, Steve Bellovin of AT&T cited an example of a company he formerly worked for that went bankrupt. He tried to track down the current owner and was unable to do so. The IANA databases still listed the owner as the bankrupt company. In a related issue, suballocations are often not recorded, which can delay the process of contacting a responsible person. For example, if there is a problem with an address with an "A" class allocation, you would know that the problem is somewhere within that organization, but not know where. If the block in question belongs to a global company like IBM, it could take days to find out who in the organization can stop the flood of packets from a particular address. Including contact information for suballocations in the IANA database would speed this process up. Fixing these problems is up to the regional address registries and their customers (ISPs). [11]

Customer-registry communication is also an are of concern. There have been a number of incidents where someone has falsified a request to change the information on a domain name, resulting in the name being routed to a bogus address. Traffic that is misdirected in this fashion is a concern because the operator of the bogus site can collect personal information (such a credit card numbers) intended for another site or cause users to download viruses or Trojan horse software. The use of secure encrypted communication in this process could reduce this risk. It is not clear, though, whether customers who do not use encryption in other types of communication will do so for this purpose. What happens, for example, to the customer who signs up for a domain name using a public key, then loses the key? Procedures to deal with such cases would be needed, but would also weaken the protection offered by encryption. [11]

Another common security threat within the DNS is "spoofing," which occurs when someone intercepts a query to a domain name server and replies with bogus information, resulting in a misdirection of the user. If the name server maintains a

record of the bogus destination and uses it to answer later queries, it is known as cache poisoning. [12,13]

The risk of spoofing and cache poisoning can be reduced fixing some well known configuration issues. However, many servers are still vulnerable. For example, several presenters cited the widespread use of obsolete versions of BIND, the most common DNS software. Presenters estimated that roughly 12 percent of the 130 million domain name servers in operation were using versions of BIND that have known security issues, mostly weaknesses that make them easy to spoof or to cause buffer overflow errors. Since these vulnerabilities can be addressed by upgrading to the current version of BIND, it is not clear why operators continue to use highly vulnerable versions, especially considering the existence of tools to exploit them and the availability of information from sources such as CERT/CC. In a related issue, it was noted that many users fail to update the root.hints file used when starting a DNS server. This file allows the server to locate the 13 root servers by address (after all, you can't do a name lookup if you don't have a working DNS server). However, although it is rare, the addresses of the 13 roots sometimes change. Users who do not keep their root.hints file up to date can send queries to addresses that no longer host root servers. In fact, one server operator stated that he still receives queries to an address that was changed several years ago. [14, 15]

Configuring servers to perform recursive queries also increases the risk of spoofing. In a recursive query, when a client queries a domain name server and the server cannot answer that query from its cache, it queries one or more servers up the DNS tree and forwards the answer to the client rather than handing off the query to the other servers. Each of packets used in a recursive query includes a tracking number. Hackers monitoring a name server can predict the next tracking number in a sequence, and send a packet with that number to spoof the response from a legitimate name server. Like the problem with obsolete versions of BIND, the risks of using recursive queries are well known, but have not been addresses on many servers. One survey by CERT/CC estimated that 80 percent of the servers it viewed were configured to allow recursion. [16]

Like other Internet servers, those running DNS services are also vulnerable to denial of service attacks. Several operators stated that by using real-time monitoring, they would be able to quickly respond to a single-source DOS attack by blocking traffic from that address. Distributed DOS attacks, however, are much more difficult to respond to. Because they are well known and there are only 13 of them, the root servers make a good target for DOS attacks. However, they are "overengineered" and as a result, DOS attacks are less likely to result in any degradation of service. [17]

Finally, several speakers pointed out that the contingency and recovery plans of most operators have not been tested. Some operators thought a live test was not worth the risk to network stability, when a catastrophic failure was unlikely. In light of September 11, however, testing of recovery for critical systems has become a higher priority. As a result, several speakers pointed out the need for additional testing, possibly including

tests by outside auditors. [18]

Responses to Vulnerabilities

Because ICANN does not run the Internet, it cannot fix all of the vulnerabilities identified. However, several areas within ICANN's responsibility were identified as possible areas of improvement:

- ICANN should consider procedures to authenticate communications, especially in emergencies.
- ICANN should mirror its IANA server to provide a live backup.
- ICANN should provide better contact information for protocol delegation.
- ICANN should test its crisis procedures.
- ICANN should conduct a detailed and public threat analysis.
- ICANN should base data backup and escrow procedures on an analysis of how long critical services can afford to be down.

ICANN also recognized the need to improve the authentication of communication between others in the DNS tree (such as user-registrar communication), but was unsure whether it should establish standards or whether it should rely on the market for a solution. The ICANN Board did not immediately take action o these recommendations. Instead, the board called for the formation of a standing committee appointed by the board president and the development of a charter for the committee. [19, 20]

Aside from ICANN, other providers of DNS services were working on responses. The IETF is in the process of implementing a best practices standard for root server security, RFC 2870. This standard broadly addresses both physical and logical security. However, the root server operators stated that compliance with this document is a goal, rather than a requirement. For example, the RFC states that a root server should perform no other function. One server, however, still maintains a country-code registry on the same machine. The root server operators were reluctant to implement more formal requirements. [21, 22, 23]

Other layers in the DNS tree are also working on best practices guidelines. Similar to RFC 2870, the TLD registries are working on a document describing the appropriate standards for physical security, as well as logical security at the data, network, and application levels. The registry document also includes standards for disaster recovery. The country-code TLDs are also working on a best practices document. A number of speakers pointed out that any new security requirements should be based on assessments of existing vulnerabilities and the trade-off with costs in money and user inconvenience. [24, 25, 26]

Summary

While the various providers of DNS services believe they are employing adequate security measures, a number of vulnerabilities still exist. Several well-known vulnerabilities have equally well-known solutions, but many DNS service providers have

not yet implemented those solutions. Other vulnerabilities, like defending against distributed denial of service attacks, do not yet have generally accepted countermeasures. ICANN and its constituency organizations are working on developing best practices documents that could enhance security, but implementation of any new procedures will have to be done with the cooperation of the operators. Also, questions about the enforceability of such standards remain unanswered.

Sources:
(NOTE: Links are mainly to presentations and notes from the November 2001 ICANN meeting. Streaming video of the presentations and discussions are also available at http://cyber.law.harvard.edu/icann/mdr2001/archive/

[1] *DNS and BIND*, Third Edition, Paul Albitz and Cricket Liu, O'Reilly, 1998, http://www.oreilly.com/catalog/dns3/chapter/ch02.html.
[2] *Department of Commerce: Relationship with the Internet Corporation for Assigned Names and Numb*ers, U.S. General Accounting Office, July 2000, http://www.gao.gov/archive/2000/og00033r.pdf
[3] Memorandum of Understanding Between the Department of Commerce and the Internet Corporation for Assigned Names and Numbers (ICANN), http://www.ntia.doc.gov/ntiahome/domainname/icann.htm
[4] ICANN, http://www.icann.org
[5] Announcement regarding ICANN's 2001 annual meeting, http://www.icann.org/announcements/announcement-26sep01.htm
[6] "Root Name Servers," Presentation by Jun Murai, 2001, http://cyber.law.harvard.edu/icann/mdr2001/archive/pres/murai.html
[7] Physical Security of the Root Name Servers," Presentation by Lars-Johan Liman, 2001, http://cyber.law.harvard.edu/icann/mdr2001/archive/pres/liman.html
[8] "DNSSec: A Short Introduction," Presentation by Olaf Kolkman, 2001, http://cyber.law.harvard.edu/icann/mdr2001/archive/pres/kolkman.html
[9] "Registry/TLD Security Panel," Presentation by Ken Silva, 2001, http://cyber.law.harvard.edu/icann/mdr2001/archive/pres/silva.html
[10] "Registrar Disaster Recovery," Presentation by Rick Wesson, 2001, http://cyber.law.harvard.edu/icann/mdr2001/archive/pres/wesson.html
[11] "ICANN and Internet Security," Presentation by Steve Bellovin, 2001, http://cyber.law.harvard.edu/icann/mdr2001/archive/pres/bellovin-keynote.html
[12] "Everything you ever wanted to know about DNS Spoofing," Johannes Erdfelt, 1997, http://www.the-project.org/admins/0797/msg00070.html
[13] "DNS Security: Present and Future," presentation by Edward Lewis, 2001, http://cyber.law.harvard.edu/icann/mdr2001/archive/pres/lewis.html
[14] "Current State of the DNS (and how to improve it)," presentation by David Conrad, 2001, http://cyber.law.harvard.edu/icann/mdr2001/archive/pres/conrad.html
[15] Scribe's notes from November 13, 2001 ICANN meeting, http://cyber.law.harvard.edu/icann/mdr2001/archive/scribe-bod-111301.html
[16] "Top Level Domain Security Checklist," presentation by Martin Lindner, 2001, http://cyber.law.harvard.edu/icann/mdr2001/archive/pres/cert.pdf
[17] Bellovin 2001, Liman 2001, and Scribe's Notes from November 15, 2001 ICANN

Meeting, http://cyber.law.harvard.edu/icann/mdr2001/archive/scribe-bod-111501.html.
[18] Scribe's Notes from the November 13 and 15, 2001 ICANN Meetings
[19] Scribe's notes from November 15, 2001 ICANN meeting.
[20] "Preliminary Report: Third Annual Meeting of the ICANN," http://www.icann.org/minutes/prelim-report-15nov01.htm

[21] "Root Name Server Operating Requirements," RFC 2870, 2000, http://www.faqs.org/rfcs/rfc2870.html.
[22] Liman 2001.
[23] Scribe's notes from November 15, 2001 ICANN Meeting.
[24] "gTLD Registry Constituency," presentation by Rita Rodin, 2001, http://cyber.law.harvard.edu/icann/mdr2001/archive/pres/rodin.html
[25] "ccTLD Registry Constituency," presentation by Peter de Blanc, 2001, http://cyber.law.harvard.edu/icann/mdr2001/archive/pres/cctld.html
[26] Scribe's notes from November 15, 2001 ICANN Meeting.